

Industry-specific

QAD SOLUTIONS

Manufacturing Applications

User Guide MFG/PRO eB2.1 New Features

Release Overview
Setting Up and Using Domains
General Ledger Consolidation
Using Q/LinQ with Multiple Domains
EDI ECommerce and Multiple Domains
Domain Reference
Users and Security
Audit Trails
Electronic Signatures



78-0608C
MFG/PRO eB2.1
January 2005

This document contains proprietary information that is protected by copyright and other intellectual property laws. No part of this document may be reproduced, translated, or modified without the prior written consent of QAD Inc. The information contained in this document is subject to change without notice.

QAD Inc. provides this material as is and makes no warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. QAD Inc. shall not be liable for errors contained herein or for incidental or consequential damages (including lost profits) in connection with the furnishing, performance, or use of this material whether based on warranty, contract, or other legal theory.

QAD and MFG/PRO are registered trademarks of QAD Inc. The QAD logo is a trademark of QAD Inc.

Designations used by other companies to distinguish their products are often claimed as trademarks. In this document, the product names appear in initial capital or all capital letters. Contact the appropriate companies for more information regarding trademarks and registration.

Copyright © 2005 by QAD Inc.
78-0608C

QAD Inc.
6450 Via Real
Carpinteria, California 93013
Phone (805) 684-6614
Fax (805) 684-1890
<http://www.qad.com>

Contents

About This Guide	1
Documentation for MFG/PRO eB2.1	2
Updated Documents for eB2.1	2
Additional Documents for eB2	3
List of Changed Topics	3
Online Help	5
QAD Web Site	6
Conventions	6
 Chapter 1 Release Overview	 9
Overview	10
Shared-Services Domain	11
Business Need	11
MFG/PRO Solution	11
Key Features	13
Menu Changes	14
Conversion	16
Database Administration	18
GL Consolidation	19
Business Need	19
MFG/PRO Solution	19
Key Features	20
New Programs	20
Modified Programs	21

Renamed Program	21
Q/LinQ	21
Business Need	21
MFG/PRO Solution	22
Key Features	23
New Programs	24
Modified Programs	24
EDI ECommerce	25
Business Need	25
MFG/PRO Solution	25
Additional Minor EDI ECommerce Changes	26
Key Features	26
New Programs	27
Modified Programs	27
Conversion	27
Security	28
Business Need	28
MFG/PRO Solution	28
Key Features	28
Modified Features	29
Menu Changes	30
Conversion	32
Enhanced Controls: Audit Trails	33
Business Need	33
MFG/PRO Solution	33
Key Features	34
New Programs	34
Modified Programs	35
Conversion	35
Enhanced Controls: Electronic Signatures	35
Business Need	35
MFG/PRO Solution	36
Key Features	36
New Programs	37
Modified Programs	37

Conversion	38
Minor Enhancements	39
Product Change Control	39
Global Tax Management Reporting	40
Sales and Use Tax Interface	42
General Ledger	42
Fixed Assets Reporting	43
AR Self-Billing Enhancement	44
Purchasing	44
Intrastat History Records	45
Service/Support Management	48
Trade Management	49
System Utilities	50
Continuing MRP/DRP Performance Improvements	50

Section 1 Domains 53

Chapter 2 Setting Up and Using Domains..... 55

Overview	56
Implementing Domains	56
Domain Setup Work Flow	57
Creating Database Records	58
Creating Domains	59
System Domain	59
Multiple Database Validations	60
Active and Inactive Domains	61
Domain Maintenance	61
Viewing Domain Information	63
Changing the Current Domain	63
Domain Access	64
Database Switching	64
Associating Domains with Sites	65
Site Connection Records	65

Setting a Default Time Zone	67
Giving Users Access to Domains	68
Configuring UI Settings	69
Setting Display Mode	69
Updating Program Information	70
Using Ctrl+F to View Information	71
Viewing Session Details	72
Setting Up Multiple Currencies	73
Defining Currencies	74
Defining Currency Accounts	74
Defining Exchange Rates	74
Defining a Source Domain	75
Calculating Derived Exchange Rates	76
Using Cross-Domain Features	79
Using Multi-Database Functions Across Domains	79
Using Features Across Domains in a Database	82
Using Domains in QAD Desktop	84

Chapter 3 General Ledger Consolidation 89

Overview	90
Consolidation Work Flows	92
Prepare Source Entities for Financial Reporting	93
Export and Import Transactions in Multiple Databases	94
Prepare Consolidation Domain	96
Defining Consolidation Sets	97
Consolidation Entities	98
Creating Consolidation Sets	98
Entity Code Maintenance	100
Viewing Consolidation Information	105
Defining Account Code Mappings	105
Consolidating Transactions	107
Validating GL Consolidation Setup	107
Consolidation Processing	107
Correcting Consolidation Transactions	108

Completing Steps after a Consolidation	109
Executing GL Consolidation	109
Viewing Transaction Detail	111
Deleting and Archiving Consolidation Sets	115
Chapter 4 Using Q/LinQ with Multiple Domains	117
Synchronizing Data	118
Data Flow	118
Synchronization Documents	122
Moving Data Between Domains	123
Data Mapping	125
Tables to Synchronize	126
Setting Up Synchronization	130
Review Tables and Fields for Synchronization	132
Define Synchronization Profiles	132
Complete Q/LinQ Setup	142
Set Up System IDs for Domains	143
Register Domains	144
Create Optional Code Mappings	149
Define Destination Lists	150
Set Up Document Specifications	152
Processing Synchronization Documents	162
Publishing Documents	163
Sending and Receiving Documents	165
Mapping and Processing Documents	167
Performing Q/LinQ Administration	167
Chapter 5 EDI ECommerce and Multiple Domains	173
Overview	174
Multiple-Domain Processing	174
Multiple-Domain Setup	176
Specifying Domain Cross-References	177
Changing the Target Domain During Transformation	178
Loading Trading Partner Library Records	179

Updating Existing User-Defined Functions	179
Chapter 6 Domain Reference	181
Non-Domain Database Tables	182
Programs that Update Cross-Domain Data	185
Default System Domain Data	188
 Section 2 Security and Enhanced Controls.	 191
Chapter 7 Users and Security	193
Security in MFG/PRO	194
Security Overview	195
Password Management	197
Basic Log-In Security	198
OS-Based Log-in Security	200
Domain Security	201
Operating System and Progress Security	201
Workstation-Level Security	205
Security Implementation Summary	208
Setting Up Security Control	213
Create a Password Strategy	219
E-Mail Notifications	222
Defining Users	223
Interaction with Licensing	224
Controlling Information Process and Display	225
Identifying Users	226
Specifying E-Mail Addresses	227
Setting Interface Preferences	228
Specifying Security Settings	229
Updating Passwords	230
Specifying Domains	231
Specifying User Groups	233
Specifying Application Use	233

Controlling Access with User Groups	234
Defining User Groups	235
User Group Example	237
Using Security Functions	238
Specifying Groups or Users	238
Assign Access by Menu	240
Limit Access to Fields	242
Control Inventory Access by Site	246
Control Entity Access	247
Define GL Account Security	248
Define Inventory Movement Code Security	249
Monitoring System Security	250
Chapter 8 Audit Trails	253
Overview	254
Auditing Process Work Flow	254
Audit Trail Data Flow	257
Electronic Signatures and Audit Databases	258
Completing Prerequisite Activities	259
Specify the OID Generator Code	259
Create and Configure Audit Databases	260
Define an Administrator Group	261
Planning an Auditing System	261
Multi-Database Environments	262
Setting Up Database Connections	263
Specifying Database Connection Parameters	265
Identifying the Database Type	266
Using a Parameter File	267
Setting Up Audit Profiles	270
Overview	270
Creating Audit Groups	271
Refreshing Profiles	272
Updating Audit Profiles	275
Activating Audit Profiles	277

Starting the Audit Process	278
E-Mail Notifications	280
Audit Profile Activation E-Mail	280
Audit Trail Creation Process Write Error	281
Audit Trail Creation Process Connection Error	281
Reporting Audit Data	282
Displaying Existing Audit Data	282
Displaying Deleted Audit Data	285

Chapter 9 Electronic Signatures 289

Overview	290
Eligible Programs	290
Electronic Signatures Work Flow	292
Categories	295
Profiles	297
Tables and Fields	298
Filters	300
Completing Prerequisite Activities	301
Set Up Audit Trails	302
Define Signature Reason Codes	302
Review Security Control Settings	303
Defining Electronic Signature Profiles	303
Overview	304
Creating Signature Groups	305
Refreshing Signature Profiles	306
Updating Signature Profiles	308
Activating Electronic Signature Profiles	315
Recording Electronic Signatures	316
Transaction Scoping	320
Product Change Control	320
E-Mail Notifications	321
Signature Profile Activation E-Mail	321
Signature Failure E-Mail	322

Reporting 322

 Setup Reports 323

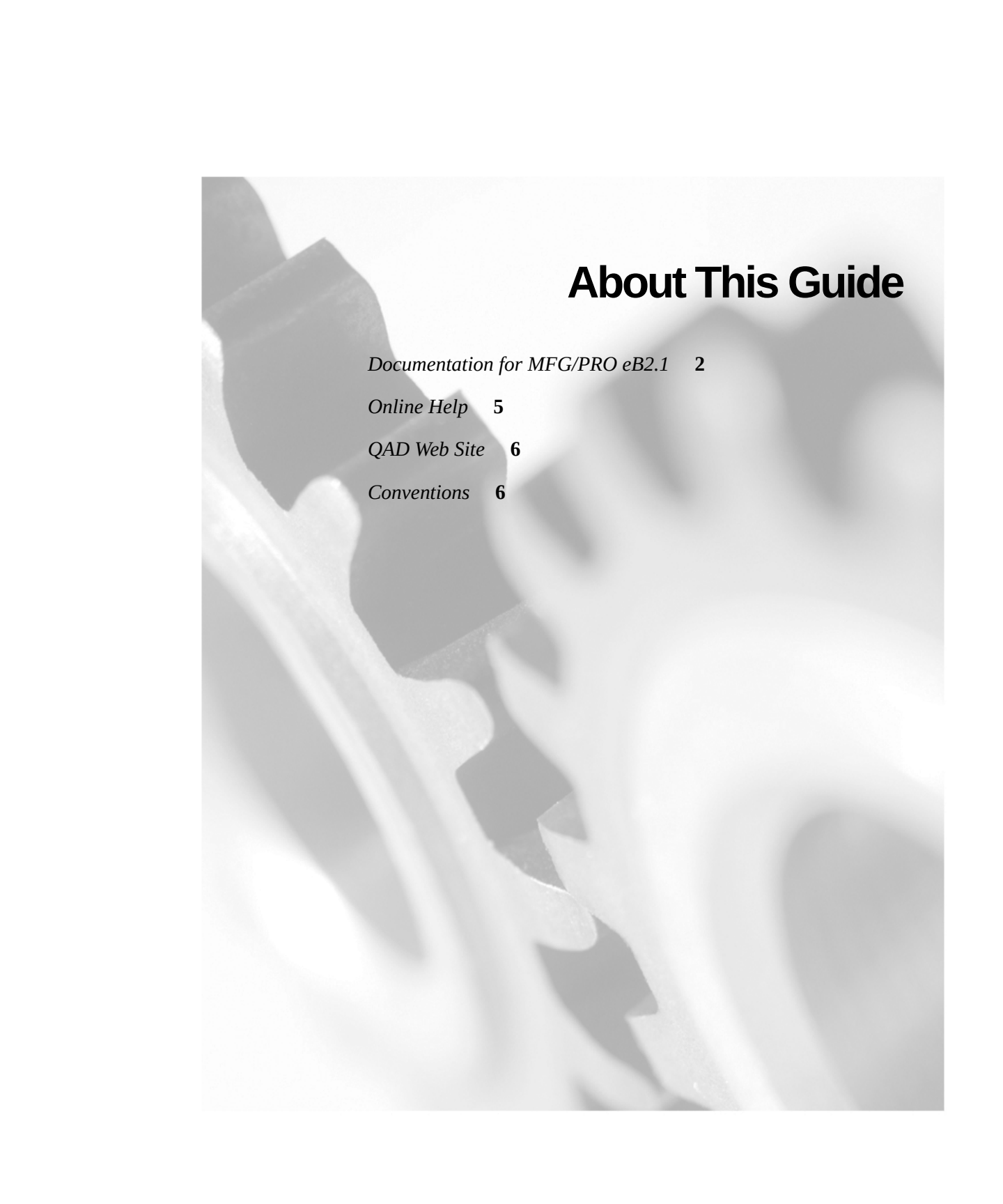
 Electronic Signature Reports 324

 Functional Reports and Inquiries 328

Archiving and Restoring Records 329

Glossary 331

Index 333

The background of the page is a grayscale image of several interlocking gears. The gears are of different sizes and are positioned in a way that they appear to be meshing together. The lighting creates highlights and shadows on the teeth of the gears, giving them a three-dimensional appearance. The overall tone is technical and industrial.

About This Guide

Documentation for MFG/PRO eB2.1 **2**

Online Help **5**

QAD Web Site **6**

Conventions **6**

This guide covers the features of the MFG/PRO eB2.1 release. Only incremental differences between MFG/PRO eB2 and MFG/PRO eB2.1 are documented in this book.

You should refer to the user guide set published for MFG/PRO eB2 for information about how unchanged functions work. The “List of Changed Topics” on page 3 indicates sections of the existing guides that have been replaced with information in this one.

Documentation for MFG/PRO eB2.1

Updated Documents for eB2.1

The following books have been updated for the MFG/PRO eB2.1 release:

- *User Guide: MFG/PRO eB2.1 New Features* includes information about all changes included in the eB2.1 release.
- *User Guide: Kanban* includes updated information on the Lean Manufacturing features included in this release. It replaces the Kanban chapter in *User Guide Volume 3: Manufacturing*.
- For software installation instructions, refer to the appropriate installation guide for your system.
- For information on installing the optional audit trails and electronic signatures features provided in the Enhanced Controls module, see *Installation Guide: Enhanced Controls*.
- For conversion information, refer to the appropriate conversion guide for your system.
- For technical details about MFG/PRO, refer to the MFG/PRO eB2.1 *Entity Diagrams* and *Database Definitions*.
- For technical details about Q/LinQ APIs, refer to *Technical Reference: Q/LinQ*.

Additional Documents for eB2

For information on other features of MFG/PRO, use the following documents:

- For information on using MFG/PRO, refer to the *MFG/PRO eB2 User Guides*.
- For instructions on navigating and using the QAD Desktop interface, see *User Guide: QAD Desktop*.
- For instructions on navigating the MFG/PRO Windows and character environments, refer to *MFG/PRO eB2 User Guide Volume 1: Introduction*.
- For information on using features that let MFG/PRO work with external applications, see the *External Interface Guides*. Each book in this set describes a separate interface such as the Sales and Use Tax application program interface (API) and Q/LinQ, the tool set for building and using data exchange tools.
- For information on QXtend Inbound, part of the QAD interoperability framework, see *Technical Reference: QXtend Inbound*.
- To view documents online in PDF format, see the *Documents on CD* and *Supplemental Documents on CD*. The CD-ROM media includes complete instructions for loading the documents on a Windows network server and making them accessible to client computers.

Note MFG/PRO installation guides are not included on a CD. Printed copies are packaged with your software. Electronic copies of the latest versions are available on the QAD Web site.

List of Changed Topics

The following table lists areas in the existing documentation set that are superseded by information in this book. Use this table to understand what information in the current set is out of date.

Guide	Chapter Number	Topic
<i>User Guide Volume 2A: Distribution</i>	Chapter 3, Global Requisition System (GRS)	New control program settings
	Chapter 8, Enterprise Material Transfer	Using EMT between domains in a single database

4 User Guide — MFG/PRO eB2.1 New Features

Guide	Chapter Number	Topic
<i>User Guide Volume 3: Manufacturing</i>	Chapter 9, Kanban	Replaced by <i>User Guide: Kanban</i>
<i>User Guide Volume 4A: Financials</i>	Chapter 2, System/Account Control	Program name, Time Zone field moved
	Chapter 3, General Ledger	Setting up entities, using multiple entities, transaction consolidation
	Chapter 5, Multiple Currencies	Defining currencies and exchange rates, consolidating multiple currency transactions, setting up account cross-references
<i>User Guide Volume 4B: Financials</i>	Chapter 3, Creating and Managing Fixed Assets	Specifying acquisition cost
<i>User Guide Volume 5: Supply Chain</i>	Chapter 14, Distribution Requirements Planning	Using DRP across domains
<i>User Guide Volume 6: Master Data</i>	Chapter 2, Items/Sites	Setting up sites and associating them with domains
	Chapter 4, Product Change Control	New security features and control program settings
	Chapter 7, Logistics Accounting	Multiple-database processing
	Chapter 8, Intrastat	Creation of purchasing and sales-related Intrastat records
	Chapter 12, Implementing GTM	New control settings
<i>User Guide Volume 7: Release Management</i>	Chapter 5, Setting Up EDI ECommerce	Setting up ECommerce to work with multiple domains
<i>User Guide Volume 8A: Service/Support Management</i>	Chapter 4, Multiple Time Zones	Location of Time Zone field, labels in service control program

Guide	Chapter Number	Topic
<i>User Guide Volume 9: Manager Functions</i>	Chapter 3, Users and Security	Controlling user access to multiple domains, as well as setting up and using enhanced security and control features; entire chapter is obsolete and replaced by the chapter in this book
	Chapter 5, Multiple Databases	Using multiple domains instead of multiple databases to implement separate business operations, changing databases
	Chapter 6, Printers and Batch Processing	Managing batch requests across domains
	Chapter 8, Database Management	Setting up time zones, dumping and loading data
	Chapter 9, Reports and Utilities	Location of operating system utilities
	Chapter 11, Application Server	Configuring application servers
<i>User Guide Volume 11: PRO/PLUS</i>	Chapter 7, Preparing to Use Self Billing	Matching invoice totals by line or by authorization number
<i>External Interface Guide: Q/LinQ</i>	Section 4, Using Q/LinQ	Synchronizing data, managing documents across domains, using destination lists

Online Help

MFG/PRO has an extensive online help system. Help is available for most fields found on a screen. Procedure help is available for most programs that update the database. Most inquiries, reports, and browses do not have procedure help.

For information on using the help system in the different MFG/PRO environments, refer to *User Guide Volume 1: Introduction* and *User Guide: QAD Desktop*.

QAD Web Site

The QAD Web site provides a wide variety of information about the company and its products. You can access the Web site at:

<http://www.qad.com>

For MFG/PRO users with a QAD Web account, product documentation is available for viewing or downloading at:

<http://support.qad.com>

You can register for a QAD Web account by accessing the Web site and clicking the Accounts link at the top of the screen. Your customer ID number is required. Access to certain areas is dependent on the type of agreement you have with QAD.

Most user documentation is available in two formats:

- Portable document format (PDF). PDF files can be downloaded from the QAD Web site to your computer. You can view them with the free Adobe Acrobat Reader. A link for downloading this program is also available on the QAD Web site.
- HTML. You can view user documentation through your Web browser. The documents include search tools for easily locating topics of interest.

Features also include an online solution database to help MFG/PRO users answer questions about setting up and using the product. Additionally, the QAD Web site has information about training classes and other services that can help you learn about MFG/PRO.

Conventions

MFG/PRO is available in several interfaces: Desktop (Web browser), Windows, and character. To standardize presentation, the documentation uses the following conventions:

- MFG/PRO screen captures show the Desktop interface.
- References to keyboard commands are generic. For example, choose Go refers to:
 - The forward arrow in Desktop

- F2 in the Windows interface
- F1 in the character interface

In the character and Windows interfaces, the Progress status line at the bottom of a program window lists the main UI-specific keyboard commands used in that program. In Desktop, alternate commands are listed in the right-click context menu.

For complete keyboard command summaries for each MFG/PRO interface, refer to the appropriate chapters of *User Guide: QAD Desktop* and *User Guide Volume 1: Introduction*.

This document uses the text or typographic conventions listed in the following table.

If you see:	It means:
monospaced text	A command or file name.
<i>italicized monospaced text</i>	A variable name for a value you enter as part of an operating system command; for example, <i>YourCDROMDir</i> .
indented command line	A long command that you enter as one line, although it appears in the text as two lines.
Note	Alerts the reader to exceptions or special conditions.
Important	Alerts the reader to critical information.
Warning	Used in situations where you can overwrite or corrupt data, unless you follow the instructions.

Release Overview

This chapter provides an overview of major updates included with MFG/PRO eB2.1.

<i>Overview</i>	10
<i>Shared-Services Domain</i>	11
<i>GL Consolidation</i>	19
<i>Q/LinQ</i>	21
<i>EDI ECommerce</i>	25
<i>Security</i>	28
<i>Enhanced Controls: Audit Trails</i>	33
<i>Enhanced Controls: Electronic Signatures</i>	35
<i>Minor Enhancements</i>	39

Overview

MFG/PRO eB2.1 introduces infrastructure for the Shared Services Domain module, allowing companies to centralize operations in fewer databases. Operations can be stored in separate, logical partitions—called *Domains*—in a single database. Each domain can have a different base currency, chart of accounts, as well as completely different configurations for manufacturing, distribution, services, and financials.

Note If you do not have a license for Shared Services Domain, the system prevents you from having more than one active domain per database.

The concept of domain greatly expands your ability to manage data for multiple related businesses with diverse business requirements. In conjunction with domains, significant changes have been made to the process of general ledger (GL) consolidation. A third major change related to Q/LinQ supports data synchronization among domains in a single database or in multiple databases.

Additionally, new security, audit trail, and electronic signature features are now available. These enhancements are designed particularly to support customers who have regulatory or legal requirements in this area, such as the requirements of Food and Drug Administration 21 CFR Part 11 and the Sarbanes-Oxley Act.

This chapter provides a high-level summary of new features included in MFG/PRO eB2.1. In addition, a number of minor enhancements are outlined in a separate section.

Information for each major feature is presented in a common format, using the following outline:

- Business need
- MFG/PRO solution
- Key features
- New menu-level programs
- Modified programs
- Conversion (if needed)

Shared-Services Domain

This release of MFG/PRO introduces a major new architectural concept into the organization of data in the MFG/PRO database that eliminates the need to manage and maintain multiple separate databases.

Business Need

MFG/PRO includes control settings that provide flexible implementation options for most manufacturing, distribution, and financial functions. However, many of these settings are database wide. For companies with multiple sites that have different operational requirements, this can limit the ability to tailor settings most effectively for each site.

In addition, each MFG/PRO database must have a single base currency and chart of accounts. This restriction makes it difficult to run multiple business operations in one database. Even though you can have more than one entity in a database, the limitation of a single currency often makes this an ineffective solution.

As a result, companies that have multiple business operations in different countries with different base currencies and GL reporting requirements must set up a separate MFG/PRO database for each. Along with making some types of reporting difficult because the data is not in one central location, this can add additional overhead and cost for IT resources needed to support these databases. A multiple-database implementation can also limit a company's ability to centralize and enforce standard practices across the enterprise.

Another related concern is data security within an enterprise. This is of particular interest to industries that are subject to regulatory requirements such as the Sarbanes-Oxley Act. Companies need to control the way users within one business operation can see or update data in another.

MFG/PRO Solution

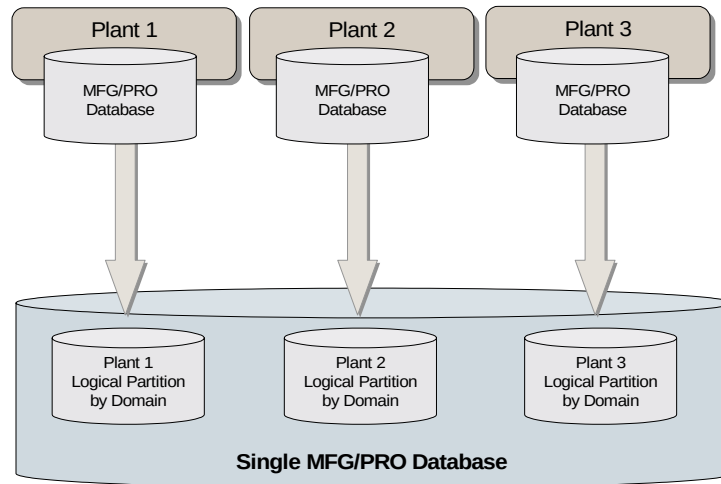
The introduction of the domain concept in the MFG/PRO database provides flexible implementation options for supporting multiple business operations within a single database and eliminates the need for a single database-wide base currency or database-wide control settings. The domain is essentially a logical partition within a single database. Any

◆ See Chapter 2, "Setting Up and Using Domains," on page 55.

number of domains can be set up in one physical database—each domain with its own base currency, chart of accounts, operating controls, document numbering, and security.

Figure 1.1 illustrates how multiple databases can be mapped into multiple domains within one database.

Fig. 1.1
Domain Solution



Note A database with one or multiple domains can continue to connect to another MFG/PRO database also with one or multiple domains.

Some system administration functions can be managed across domains, such as defining users, currency codes, country codes, menus, messages, and labels. This includes the ability for a system administrator to control exactly which users can access data in which domains. All other data updates take place within the context of a specific domain.

Replication tools let system administrators synchronize common master data across domains, where appropriate. Processes that currently operate between databases can be used between domains within a database in a more streamlined and reliable manner. These processes include distribution requirements planning (DRP), enterprise material transfer (EMT), and enterprise operations planning.

Combining operations in a single database can have the following advantages:

- Facilitate the standardization of business processes among operational units.
- Reduce IS costs as a result of having fewer databases to manage.
- Facilitate reporting and custom queries because all data is stored in the same table structure referenced by the domain field.
- Support data sharing.

Each business can choose the most appropriate deployment method:

- A solution with a different database for each business operation
- A central solution with one database serving all
- Any combination of these

Key Features

Using features of domain, you can:

- Set up domains and associate domains with databases.
- Specify a default domain for each user and assign each user access to one or more domains by user group. Based on the associated user group, a user can have access to different menu functions in each assigned domain.
- Switch domains as needed to another domain that you have access to. When the new domain resides in another database, initiate database switching as well.
- View the active domain and base currency on each MFG/PRO screen based on configurable settings.
- Set up system-wide data that applies to all domains, such as users, e-mail definitions, printers, country codes, and interface information such as menus, messages, and label data.
- Synchronize master data such as item and address records across various domains within a database using synchronization tools provided with Q/LinQ.
- Create a primary site—one that contains inventory records—in one domain and automatically create corresponding connection sites in other domains and connected databases.

♦ See “Q/LinQ” on page 21.

- Use features of Enterprise Material Transfer (EMT) across business units represented by domains within a database as well as with business units in external databases.
 - Use Distribution Requirements Planning (DRP) with sites belonging to different domains within a database as well as with sites in external databases.
- ◆ See page 25.
- ◆ See page 21.
- Use one instance of EDI ECommerce to serve multiple domains.
 - Use one instance of Q/LinQ to serve multiple domains.
 - Manage batch jobs for multiple domains in Batch Request Detail Maintenance (36.14.3) and Batch Request Processor (36.14.13).
 - Set up currency codes for the database and define currency accounts for each domain.
 - Define exchange rates in one source domain and calculate derived exchange rates in other domains that are related to the source.
 - Specify a time zone for the database server in a new Database Control (36.24) program.
 - View transactions across domains using two new reports: Transaction Numbering Report (3.21.19) and Operations Numbering Report (17.13.22, 18.4.16, 18.22.4.12).

Menu Changes

Changes introduced to support domains have added programs to the menu, deleted programs, renamed programs, and moved programs. The tables in this section provide details of these changes. An additional table lists programs that display changes to the user interface.

New Programs

Table 1.1 lists the new programs added to MFG/PRO to support domains.

Table 1.1
New Domain
Programs

Menu Number	Description	Program Name
3.21.19	Transaction Numbering Report	ictnrp.p
17.13.22	Operations Numbering Report	reopnrp.p
18.4.16		
18.22.4.12		

Menu Number	Description	Program Name
26.7	Currency Account Maintenance	mccuacmt.p
26.8	Currency Account Browse	mcbr008.p
26.10	Exchange Rate Relationship Maintenance	mcdexrmt.p
26.11	Exchange Rate Relationship Browse	mcbr010.p
26.12	Derived Exchange Rate Calculation	mcderccp.p
36.10.1	Domain Maintenance	mgdommt.p
36.10.2	Domain Browse	mgbr225.p
36.10.3	Domain Report	mgdomrp.p
36.10.13	Change Current Domain	mgdomchg.p
36.14.4	Batch Request Detail Browse	mgbr227.p
36.24	Database Control	mgdbpm.p

Modified Programs

The addition of domains to the database has affected most database tables and as a result, most programs in MFG/PRO. These changes allow the programs to find records based on a domain value. Otherwise, the way most programs appear to the user and the way they function has not changed.

You will see changes to the interface of the programs listed in Table 1.2.

Menu Number	Description	Program Name
1.1.13	Site Maintenance	icsimt.p
26.1	Currency Maintenance	mccumt.p
36.1	Domain/Account Control	mgglpm.p
36.3.21.1	Program Information Maintenance	mgpgmimt.p
36.3.24	Security Control	mgurpmmt.p
36.14.3	Batch Request Detail Maintenance	mgbcdmt.p
36.14.5	Batch Request Detail Report	mgbcdrp.p
36.14.13	Batch Request Processor	mgbatch.p
36.20.10.15	Session Master Maintenance	mgssesmt.p

Table 1.2
Programs Modified
for Domain

Deleted Programs

With the introduction of domains, the program listed in Table 1.3 is obsolete.

Table 1.3
Deleted Program

Menu Number	Description	Program Name
36.6.17	Current Database Change	mgdccg.p

Moved Programs

The menu and programs listed in Table 1.4 have been moved to accommodate changes introduced with domains.

Table 1.4
Moved Programs

Old Menu Number	New Menu Number	Description	Program Name
36.24	36.22	Operating Systems Command Menu	
36.24.1	36.22.1	Exit to Operating System	mgoscall.p
36.24.3	36.22.3	Program Execute	mgmgmt24.p
36.24.4	36.22.4	Program/Text File Display	mgfdsply.p
36.24.13	36.22.13	Disk Space Inquiry	mgdfds.p

Renamed Program and Menu

The following menu items have been renamed to more accurately reflect their purpose in a multi-domain environment:

- System/Account Control (36.1) has been renamed Domain/Account Control since the settings you define with it apply to each domain individually, not across the entire system.
- System Constants Menu (36.2) has been renamed Domain Constants Menu since the codes you define with it apply to specific domains, not across the system.

Conversion

The addition of domains to the database has affected most database tables. When you upgrade to a release of MFG/PRO containing domains, a conversion is required. This conversion is fully documented in the conversion guide for your system.

The conversion completes the following tasks:

- Create a system domain named QAD and load default data into it.
- In a single database environment, create a connection record for qaddb and prompt for a domain code, name, and short name for the current working database. The conversion creates a domain record representing that database based on the values you supply and loads data from the source database into it.
- In a multi-database environment, display a list of databases found in Database Connection Maintenance (36.6.1) and prompt for the conversion database. Then prompt for domain code, name, and short name for each defined database. The conversion creates these domains and replaces the database name currently referenced on site records with the appropriate domain code.
- Update the Domain field in all converted tables with the domain you specify.
- Give each user defined in the database access to the domain representing the converted database. Any security group information currently associated with the user is also associated with the domain.
- Move accounts associated with currencies to the account defaults table in the database.
- Move the server time zone data from Domain/Account Control (36.1) to the new Database Control (36.24) table.
- Update the value of the new Multi Domain field maintained with Program Information Maintenance (36.3.21.1) for QAD-supplied programs.

If you have custom code that you need to convert, you should contact QAD Global Services for help in the conversion. Global Services can also provide help with implementation planning if you want to take advantage of the domain infrastructure by merging existing databases into separate domains within a single database.

To support both current features such as the optional Enhanced Controls module as well as future development, each database table is also converted to add a field for recording a unique object ID (OID). This field is used to identify the record for auditing and other purposes. During conversion, you specify an OID generator code used to populate the OID fields. You must specify this code during a new installation also.

Database Administration

Managing a database with domains is essentially the same as managing databases in previous releases of MFG/PRO. However, you should be aware of the effect of domains in the following areas:

◆ See Chapter 4, “Using Q/LinQ with Multiple Domains,” on page 117.

◆ See “Viewing Transaction History Across Domains” on page 82.

◆ For additional details, see the installation guide for your system.

- Delete/archive functions exist for most record types in MFG/PRO. In previous releases of MFG/PRO, data created with an archive function could be loaded into another database to populate tables. This alternate use of archived data is no longer possible, since most data is now domain specific. You can use the data replication tools provided with Q/LinQ to synchronize master data among domains and databases.
- Sequences are database constructs used to generate sequence numbers for a number of MFG/PRO programs. Sequences apply to an entire database and are not domain specific. As a result, sequence numbers may appear to have gaps within a particular domain when a database has more than one domain. Two new reports let you view sequence numbers across domains to confirm that gaps do not exist in the database.
- Triggers apply to all databases accessing the same MFG/PRO source code, and thus to all domains within a database. They cannot be customized per database or per domain.
- In a multi-language installation, each domain in a database can have a different default language. The appropriate language setting can then be defined using client startup parameters or encoding settings. However, it is possible that some combination of languages may still require separate databases to resolve code page issues.

GL Consolidation

This release of MFG/PRO introduces significant enhancements to the GL consolidation process.

Business Need

Consolidation is typically used when multiple entities must report financial statements in one currency or using a common chart of accounts. Prior to this release of MFG/PRO, entities with different base currencies had to exist in separate databases. This requirement created additional operational overhead in environments that used financial shared services.

Producing consolidated financial reports required exporting transactions from one database and importing them into a consolidation database. This activity can extend the time needed to complete business-critical period-end reporting. In addition, consolidation was error-prone, since no controls or validation existed on the import process.

MFG/PRO Solution

The addition of the domain concept supports enhanced and streamlined GL consolidation among entities within a domain and between entities in different domains. Before initiating consolidation, you create one or more consolidation sets that determine which subsidiary entities should be included as well as how the transactions should be apportioned and summarized.

The use of consolidation sets prevents errors and streamlines the consolidation process. You can optionally create consolidation sets to facilitate multiple reporting views of a business.

You can run consolidation in a preview mode to avoid errors; you can also reprocess failed transactions after correcting errors.

After consolidation, you can use reports to drill down from a consolidation transaction to the actual transaction detail in the subsidiary entity.

► See Chapter 3, “General Ledger Consolidation,” on page 89.

Key Features

Using features of GL consolidation, you can:

- Set up account cross-reference information to be used with GL consolidation as well as transaction import.
- Create multiple consolidation sets that specify which entities are combined for GL consolidation and other parameters that control how the consolidation occurs.
- Define hierarchical relationships among entities, with lower-level business units consolidating into higher-level units at multiple levels.
- Define proportional consolidation when transactions from one business unit should consolidate into multiple consolidation entities or when you need to consolidate financial results for associated companies or non-fully owned subsidiaries.
- Consolidate GL transactions across domains within a database as well as with external databases.
- Create consolidation sets that are used primarily for modeling and reporting.
- Delete and/or archive consolidated transactions and consolidation sets when they are no longer needed.
- Use Inquiry by Account with Drill Down (25.13.20) to view source transaction detail for consolidation transactions, down to the original transaction in the source domain.

New Programs

Table 1.5 lists new programs added to MFG/PRO to support GL consolidation.

Table 1.5
New GL
Consolidation
Programs

Menu Number	Description	Program Name
25.3.1.6	Consolidation Entity Delete/Archive	glenu.p
25.19.10	Entity Consolidation Detail Inquiry	glencdiq.p
25.19.11	Entity Consolidation Detail Report	glencdrp.p
25.19.20	GL Consolidation	gltrdcs.p

Modified Programs

You will see changes to the interface of the programs listed in Table 1.6. In some cases, the appearance of programs has not changed, but the way you use them has. This is true of most of the programs on the Transaction Import/Export menu (25.19). The chapter on GL consolidation provides details about how these programs are now used.

See Chapter 3, “General Ledger Consolidation,” on page 89.

Menu Number	Description	Program Name
25.3.1.1	Entity Code Maintenance	glenmt.p
25.3.1.2	Entity Code Browse	gpbr322.p
25.13.11	Transaction Summarization	glcons.p
25.13.20	Inquiry by Account with Drill-Down	gltriq2.p
25.19.4	From-Account Cross-Reference Maintenance	glacxfmt.p
25.19.6	From-Account Cross-Reference Report	glacxrp.p
25.19.14	Transaction Export	gltrexp.p

Table 1.6
Programs Modified
for GL
Consolidation

Renamed Program

Transaction Consolidation (25.13.11) has been renamed Transaction Summarization to avoid confusion with the new GL Consolidation (25.19.20) program.

Q/LinQ

Q/LinQ is QAD’s tool set for building integrations with other applications. Q/LinQ provides infrastructure for administering and managing data exchange between MFG/PRO and external applications. This same infrastructure supports data exchange both between domains in connected MFG/PRO databases and between domains within a single database.

Business Need

The introduction of domains in this release of MFG/PRO means that separate business operations can now be managed in a single database. Many of the issues related to distributed operation now apply to managing information in separate domains. For example, domains may share key

master data such as items and addresses. Maintaining this data separately is inefficient and error prone. A way to synchronize this data needs to be provided.

In addition, Q/LinQ previously assumed that a database represented one corporate entity. Q/LinQ needs to be enhanced to support multiple identities within one database, but allow the administration of document import and import to take place across domains.

◆ See *Technical Reference: QXtend Inbound* for details.

Q/LinQ also needs to be enhanced to support QXtend Inbound. QXtend Inbound is a component of the QAD QXtend interoperability framework, which provides a single, standardized data interface between QAD products and between QAD products and external systems. The interface is a Web services-based, SOAP-compliant, XML framework, enabling complete platform-independent access to MFG/PRO business functionality.

◆ See “Glossary” on page 331 for definitions of unfamiliar terms and abbreviations.

The first release of QXtend Inbound delivers inbound data to MFG/PRO menu-level programs. The inbound data is in the form of XML data documents, called QDocs, delivered using a user interface (UI) API adapter or, for a select few programs, a code API adapter.

MFG/PRO Solution

◆ See Chapter 4, “Using Q/LinQ with Multiple Domains,” on page 117.

The Data Synchronization (DataSync) functions, previously available as a separate QAD product, have been incorporated into Q/LinQ in this release of MFG/PRO. The synchronization features of Q/LinQ have been enhanced to ensure that static data—such as sites, item numbers, customer addresses, and GL accounts—exactly correspond among multiple domains in a single database as well as among multiple, distributed MFG/PRO databases.

The system captures data changes that are then transmitted to other domains and databases using Q/LinQ export and forwarding features. When the destination is another database, documents are published and sent using source Q/LinQ features and received, mapped, and processed using Q/LinQ in the destination database. When the destination is another domain in the same database, the process is streamlined. Documents in the source domain are published directly to the import queue of the destination domain, where they are mapped and processed to complete the table updates.

In a multi-domain installation with extensive sharing of master data, it may be necessary for particular database updates in each domain to be propagated to many other domains. To streamline the setup required to support this scenario, a new function has been added to Q/LinQ that lets administrators copy import and export specifications from any domain to their current working domain. This lets them create template specifications that can then be copied and reused with only minor changes. The search logic Q/LinQ uses to find specifications has been changed to let administrators define more generic templates, also streamlining the setup process.

In addition, a number of Q/LinQ function have been enhanced to operate either for one domain or for all domains. This streamlines administration in a multi-domain environment where support for integrations is centralized. For example, administrators can delete and/or archive documents across all domains.

To support QXtend Inbound, you can now specify the location of the QXtend server and indicate during import if a document should be processed using QXtend. Q/LinQ APIs have been enhanced with new methods to process the XML QDoc message format.

◆ See *Technical Reference: Q/LinQ* for details about API changes.

Key Features

Using the enhanced features of Q/LinQ, you can:

- Create synchronization profiles detailing tables and fields to be synchronized and share these profiles with all domains in a database.
- Define one-to-one, one-to-many, and many-to-many synchronization relationships among source and destination domains in a single database or multiple databases.
- When synchronizing data, define lists of domains or external databases and associated domains to receive exported documents, rather than exporting separately to each.
- Use an adapter provided with Q/LinQ to communicate changes or choose any other Q/LinQ supported method to communicate changes for synchronization among databases: file write/read, Q/LinQ stream API, or Q/LinQ messaging APIs.
- Define default import and export specifications that apply to all applications and trading partners.

- Copy import or export specifications from a source domain to your current working domain, streamlining the creation of similar specifications.
- Execute Q/LinQ administrative tasks for one domain or all domains. This includes processing documents, reporting on documents, dumping documents to file, and deleting and archiving documents.
- Import QDocs and process the XML messages generated from QXtend Inbound.

New Programs

Table 1.7 lists programs added to Q/LinQ to support data synchronization and cross-domain administration.

Table 1.7
New Q/LinQ
Programs

Menu Number	Description	Program Name
36.8.1.4	Export/Import Specification Copy	qqspeccp.p
36.8.1.5	Export/Import Specification List	qqspclst.p
36.8.8	Destination List Maintenance	qqdalmt.p
36.8.22	Data Synchronization Setup Menu ...	
36.8.22.1	Synchronization Profile Maintenance	qqsypmt.p
36.8.22.2	Synchronization Profile Inquiry	qqsypiq.p
36.8.22.3	Sync Table–Field Maintenance	qqsytfmt.p
36.8.22.4	Sync Table–Field Browse	qqbr030.p
36.8.22.8	Synchronization Mass Export	qqsymsex.p

Modified Programs

The addition of domains to the database has affected most database tables and as a result, most programs in Q/LinQ. These changes allow the programs to find records based on a domain value. Otherwise, the way most Q/LinQ programs appear to the user and the way they function have not changed.

However, some Q/LinQ reports and administrative functions have been enhanced so that users can view and manage documents from multiple domains.

You will see changes to the interface of the programs listed in Table 1.8.

Menu Number	Description	Program Name
36.8.10	Process Import Documents	qqimprc.p
36.8.16	Export/Import Document Query	qqbr.p
36.8.17	Export/Import Document Report	qqierp.p
36.8.18	Dump Export/Import Documents to File	qqwrt.p
36.8.23	Export/Import Document Delete/Archive	qqrup.p

Table 1.8
Q/LinQ Programs
Modified for
Domain

EDI ECommerce

EDI ECommerce is the advanced electronic data interchange (EDI) interface between MFG/PRO and third-party EDI communications or translator products, sometimes referred to as electronic commerce (EC) subsystems.

Business Need

The introduction of domains in this release of MFG/PRO means that separate business operations can now be managed in a single database. To take full advantage of this feature, EDI ECommerce users require the flexibility to have a single instance of that product import and export documents between multiple MFG/PRO domains and the EC subsystem.

Additionally, users need the ability to reduce setup time by being able to centralize static EDI setup data and make it available to all domains.

MFG/PRO Solution

The multiple-domain features of EDI ECommerce allow flexibility in how you can set up import and export processing.

EDI ECommerce has been updated in the current release to provide shared document import and export services across multiple domains while allowing single-point entry of a significant amount of common setup data.

◆ See Chapter 5, “EDI ECommerce and Multiple Domains,” on page 173.

Additional Minor EDI ECommerce Changes

As part of the ongoing EDI ECommerce interoperability enhancements, a new program has been added and new fields have been added to the existing programs:

- Sales order packing lists can now be exported using Packing List Export (35.4.15). This exported document can be used to indicate a request for shipment of product from a public warehouse to a customer location.
- In Exchange Definition Maintenance (35.15.6) and Implementation Definition Maintenance (35.15.13), new fields let you add a namespace reference for document definitions related to XML. Separate fields are available at the record and field levels.
- In Transmission Group Maintenance (35.13.13), you can now specify a timeout parameter for the HTTP server used for posting messages to the transmission group.

Key Features

Using the enhanced features of EDI ECommerce, you can:

- Run EDI ECommerce in a single domain and still be able to export documents from and import them into multiple domains as needed.
- Run EDI ECommerce in more than one domain while sharing certain data-intensive records used to map information between MFG/PRO and the external EDI subsystem.
- Allow for differences between domains based on domain-specific data, such as control program records and repository data created during document import and export.
- Cross-reference a user's log-in domain to the domain used in EDI ECommerce processing.
- Use an EDI ECommerce program to switch the processing domain during an EDI session.

New Programs

Table 1.9 lists the programs added to EDI ECommerce.

Menu Number	Description	Program Name
35.4.15	Packing List Export	edompick.p
35.11	ECommerce Domain Menu	
35.11.1	Domain Cross Reference Maintenance	eddmnmt.p
35.11.11	Change Current ECommerce Domain	eddomchg.p

Table 1.9
New EDI
ECommerce
Programs

Modified Programs

Programs throughout EDI ECommerce have been updated to recognize domain values used during document processing, including transformation function programs and the gateway programs that move data into and out of the MFG/PRO database.

Additionally, the programs shown in Table 1.10 have been modified to add domain-related fields to the user interface.

Menu Number	Description	Program Name
35.9.17	Turnaround Data Maintenance	edtarmt.p
35.9.19	Turnaround Data Report	edtarrp.p
35.17.7	Trading Partner Library Load	edtpload.p
35.17.19	Turnaround Data Archive/Delete	edtararc.p

Table 1.10
Modified EDI
ECommerce Menu
Programs

Conversion

Installing MFG/PRO eB2.1 adds a new DOMAIN token to EDI ECommerce. Because this token may be used by transformation functions, you must manually update any user-defined functions that existed before the current release.

◆ See “Updating Existing User-Defined Functions” on page 179.

Note QAD-defined functions are updated during installation.

Security

▶ See “Users and Security” on page 193.

Several new security features have been added to MFG/PRO to increase the access-control options available to system administrators—particularly when they are tasked with meeting the security requirements of external regulatory agencies.

Business Need

Many companies must adhere to strict security procedures—both those required by internal corporate policies and those specified by such governing bodies as the U.S. Food and Drug Administration (FDA). Meeting these needs requires more robust and configurable security features to maintain a stable and secure MFG/PRO environment.

MFG/PRO Solution

The enhanced security features in MFG/PRO give you increased control over system access at several points, including log-in, domain change, the menu system, and such elements as sites and GL accounts. Enhancements include a much more robust set of tools for assigning and controlling user passwords, as well as tracking and monitoring user access.

The new features can be used along with available operating system and Progress tools to provide a more comprehensive approach to security in a regulated environment.

Key Features

With the enhanced MFG/PRO security features, you can:

- Validate that the entered log-in ID is an active user.
- Maintain detailed log-in date and time history.
- Create and enforce log-in rules, such as disabling a user account for too many failed log-in attempts.
- Manually deactivate user accounts when they are no longer needed, and specify a reason code each time the active status is updated.

- Set up automatic e-mail alerts to system administrators for abnormal security events, such as a user account being deactivated for too many failed log-in attempts.
- Display warning messages to alert users to impending password expiration, and allow them to change their passwords following the warning messages.
- Create user groups and add or remove users from these groups as needed.
- Assign security to menus, sites, GL accounts, and so on using previously defined, validated groups.
- Force password changes by user, user group, or system wide based on the date of the last password change.
- Manually assign temporary passwords to users, or automatically generate new passwords.
- Optionally have the system e-mail auto-generated temporary passwords directly to users, to prevent even the system administrator from ever knowing the password.
- Set up password composition parameters, such as length and minimum letter and number usage.
- Display the system date or the user name on all MFG/PRO screens.

Modified Features

The following MFG/PRO features have been modified with the introduction of the new features:

- In GUI environments, users can no longer save their user IDs at the log-in screen.
- User Option Telnet Maintenance (36.20.10.4) no longer displays the user password. The password must now be entered twice for verification.
- The user and user group lists maintained by several MFG/PRO security programs are now validated against:
 - Groups defined in the new User Group Maintenance (36.3.4) program
 - User IDs set up in User Maintenance (36.3.1)

An error displays if you attempt to add an invalid user group or user ID in any of the following programs:

- Tax Interface Control (2.13.23.24)
- Menu Security Maintenance (36.3.10)
- Site Security Maintenance (36.3.15)
- GL Account Security Maintenance (36.3.16)
- Inventory Movement Code Security (36.3.17)

Menu Changes

New Programs

Table 1.11 lists the programs added to MFG/PRO to support the new security features.

Table 1.11
New Security
Programs

Menu Number	Description	Program Name
36.3.4	User Group Maintenance	mgurgpmt.p
36.3.5	User Group Inquiry	mgurgpiq.p
36.3.23	Reports and Utilities Menu	
36.3.23.1	Logon Attempt Report	mgurpsrp.p
36.3.23.2	User Account Status Report	mguactrp.p
36.3.23.4	User Group Report	mgurgprp.p
36.3.23.12	User Password Force Change Util	utfrcpsw.p
36.23.3	Logon History Archive Delete	mguslhup.p

Modified Programs

Table 1.12 lists the programs that have been modified to support the new security features.

Table 1.12
Modified Security
Programs

Menu Number	Description	Program Name
36.3.1	User Maintenance	mgurmt.p
36.3.2	User Inquiry	mguriq.p
36.3.3	User Password Maintenance	mgurmt.p
36.3.10	Menu Security Maintenance	mgpwmt.p

Menu Number	Description	Program Name
36.3.11	Menu Security Change	mgpwcg.p
36.3.24	Security Control	mgurpmmt.p
36.17.6	Control Tables Report	mgpmp.p
36.20.10.3	User Option Telnet Maintenance	mgusrtmt.p
36.20.10.4	User Option Report	mgusrp.p

Updated Menu Structure

Most programs on the Security Menu were moved to different menu locations to accommodate the new programs. Table 1.13 illustrates the new menu structure.

Menu Number	Description	Program Name
36.3.1	User Maintenance	mgurmt.p
36.3.2	User Inquiry	mguriq.p
36.3.3	User Password Maintenance	mgurmt.p
36.3.4	User Group Maintenance	mgurgpmt.p
36.3.5	User Group Inquiry	mgurgpiq.p
36.3.10	Menu Security Maintenance	mgpwmt.p
36.3.11	Menu Security Change	mgpwcg.p
36.3.13	Entity Security Maintenance	glsecmt.p
36.3.14	Entity Security Inquiry	glseciq.p
36.3.15	Site Security Maintenance	clsismt.p
36.3.16	GL Account Security Maintenance	mgacsmt.p
36.3.17	Inventory Movement Code Security	sosimt.p
36.3.18	Inv Mvmt Code Security Browse	gpbr502.p
36.3.19	Field Security Maintenance	mgflpwmt.p
36.3.20	Field Security by Group	mgflgpmt.p
36.3.22	User Access by Application Inquiry	lvusrpq.p
36.3.23	Reports and Utilities Menu	
36.3.23.1	Logon Attempt Report	mgurpsrp.p
36.3.23.2	User Account Status Report	mguastrp.p
36.3.23.4	User Group Report	mgurgprp.p
36.3.23.12	User Password Force Change Util	utfrpcsw.p

Table 1.13
Updated Security
Menu

Menu Number	Description	Program Name
36.3.23.13	Entity Security Report	glsegrp.p
36.3.23.15	Site Security Report	clsisrp.p
36.3.23.16	GL Account Security Report	mgacsrp.p
36.3.23.19	Activated Field Security Report	mgflpwrp.p
36.3.23.20	Dictionary Field Security Report	mgfldcrp.p
36.3.24	Security Control	mgurpmmt.p

Conversion

Several new fields and tables have been added to MFG/PRO to support the security enhancements. Highlights of the conversion process include the following:

- User Maintenance no longer lets you define a blank user ID. If a blank user ID is detected during the conversion, it is retained in the database for historical purposes. However, you cannot update the record in User Maintenance after the conversion, and the conversion routine sets the Active field to No.
- User Maintenance has a new mandatory field, Active Reason, for identifying the reason for changing the user's active status. The conversion populates this field with the default reason code QAD_DEF, which is associated with the reason type User_Act used by security functions.
- To support the new user group feature, the conversion searches for user groups previously entered in comma-separated lists in User Maintenance and creates a record for each in the user group master table. It then adds the associated user as a member of the group for the production domain specified during the domain conversion.
- For additional security, the password associated with telnet log-in scripts in User Option Telnet Maintenance (36.20.10.3) is now encrypted. The conversion encrypts any existing passwords.

Enhanced Controls: Audit Trails

This release of MFG/PRO introduces a major enhancement—the optional, separately installed Enhanced Controls module—that allows companies to track in detail who made changes to enterprise-critical data, what changes were made, and when.

Enhanced Controls includes two functional areas:

- Audit trails, described in this section
- Electronic signatures, described in the subsequent section ▶ See page 35.

Business Need

Control of electronic transactions is a major concern for all businesses. Companies require a tool set that enables them to maintain detailed records of their business system transactions; in many environments, electronic record-keeping activities must meet strict accountability requirements set forth by governing bodies. The current audit trail features in MFG/PRO are very limited in scope and apply to only some transactions.

▶ See Chapter 8, “Audit Trails,” on page 253.

MFG/PRO Solution

Use the Enhanced Controls audit trail functions to maintain multiple separate audit databases containing a history of changes made to records associated with the MFG/PRO database tables you choose. Audit trail records include data such as:

- Identifying information for the user performing the update
- Date, time, and time zone when the change was posted
- Before and after data values for changes, additions, and deletions

The audit trail functions use a new object ID field that has been added to all MFG/PRO database tables. This field is used to uniquely identify, link, and track each MFG/PRO database record with audit trail information maintained in the audit trail database.

Key Features

Using audit trail features, you can:

- Automatically create detailed audit trail records of changes made to any audit-enabled database table.
- Maintain audit trail information in single and multiple-database environments.
- Trace change history for all or a few selected database tables.
- Group audit profiles to quickly update, activate, or deactivate tracking for multiple tables simultaneously.
- Trace changes by date and time.
- Maintain and report against one or a range of audit databases.
- Use e-mail functions to automatically notify system administrators when audit configurations change or when problems occur with the audit trail process.

New Programs

Table 1.14 lists new programs added to MFG/PRO as part of the Enhanced Controls module to support audit trail functions.

Table 1.14
New Enhanced
Controls Programs

Menu Number	Description	Program Name
36.12	Enhanced Controls Menu	
36.12.1	Audit Trail Report – Existing	atexpr.p
36.12.2	Audit Trail Report – Deleted	atdelrp.p
36.12.13	Audit Trail Setup Menu	
36.12.13.1	Audit Trail Group Maintenance	attgmt.p
36.12.13.2	Audit Trail Group Report	atgrrp.p
36.12.13.4	Audit Workbench Refresh	atwpref.p
36.12.13.5	Audit Workbench Profile Maintenance	atwpmt.p
36.12.13.6	Audit Workbench Profile Report	atwprp.p
36.12.13.8	Audit Profile Activation	atwpact.p
36.12.13.9	Activated Audit Profile Report	ataprp.p
36.12.13.11	Audit DB Maintenance	atdbmt.p
36.12.13.12	Audit DB Report	atdbrp.p

Menu Number	Description	Program Name
36.12.13.23	Audit Trail Creation Process	atttpui.p
36.12.13.24	Audit Trail Control	atpm.p

Modified Programs

Table 1.15 lists existing programs modified to support audit trail functions.

Menu Number	Description	Program Name
36.24	Database Control	mgdbpm.p

Table 1.15
Modified Programs

Conversion

To use the audit trail functions, the MFG/PRO database must be updated during the implementation by activating audit trail required database triggers. Details for completing this task are included in *Installation Guide: Enhanced Controls*.

Enhanced Controls: Electronic Signatures

This release of MFG/PRO adds electronic signature capabilities to let you require a user to enter a valid user ID and password, as well as a reason code, when creating or updating records in key MFG/PRO programs.

This feature is part of the optional, separately installed Enhanced Controls module.

Business Need

As part of an overall approach to meeting the user accountability requirements of regulatory bodies, companies need additional access and tracking controls that require users of certain critical programs to electronically sign records.

See Chapter 9, “Electronic Signatures,” on page 289.

► See “Eligible Programs” on page 290.

MFG/PRO Solution

Use the electronic signature functions of the Enhanced Controls module to apply electronic signature requirements to a subset of menu programs and MFG/PRO database tables you choose from QAD-provided default setup data. Signature records include data such as:

- Identification of the user who created or modified the data
- An indication of whether the data has been updated since it was most recently signed
- Remarks the user entered when signing the data
- Detailed field values for all elements of the signature record

Key Features

Using electronic signature features, you can:

- From QAD-provided category definitions, set up profiles that specify subsets of programs and database fields used with electronic signatures in your specific environment.
- For each category profile, specify whether the latest signature displays when the user starts a program, as well as whether the system generates final transactions before displaying the data to be signed.
- Define custom reason codes to describe the exact meaning of the signature in your environment.
- Group category profiles to quickly update, activate, or deactivate signature functions for multiple profiles simultaneously.
- Use e-mail functions to automatically notify system administrators when a user unsuccessfully attempts to enter a signature more than a specified number of times, as well as when signature profiles are activated.
- Generate reports on electronic signature events, as well as detailed lists of field values included in the signed data.
- Archive signature records to an online audit database.

New Programs

Table 1.16 lists new programs added to MFG/PRO as part of the Enhanced Controls module to support electronic signature functions.

Menu Number	Description	Program Name
36.12.4	E-Signature Events Report	esevtrp.p
36.12.5	E-Signature History Report	eshstrp.p
36.12.7	E-Signature Failure Report	esflrp.p
36.12.14	E-Signature Setup Menu	
36.12.14.1	E-Signature Group Maintenance	escgmt.p
36.12.14.2	E-Signature Group Report	esgrrp.p
36.12.14.4	E-Signature Workbench Refresh	eswpref.p
36.12.14.5	E-Sig Workbench Profile Maint	eswpmt.p
36.12.14.6	E-Sig Workbench Profile Report	eswprp.p
36.12.14.8	E-Signature Profile Activation	eswpact.p
36.12.14.9	Activated E-Sig Profile Report	esacrp.p
36.12.14.11	E-Sig Category Master Report	escatrp.p
36.12.14.21	E-Sig Failure Archive/Delete	esesigup.p
36.12.14.22	E-Signature Archive/Delete	esesup.p
36.12.14.23	E-Signature Restore	esesld.p

Table 1.16
New Electronic
Signatures
Programs

Modified Programs

Table 1.17 lists existing programs modified to support electronic signature functions.

Menu Number	Description	Program Name
1.22.1	Lot Master Maintenance	clltmt.p
1.22.2	Lot Master Inquiry	icltmiq.p
1.22.24	Compliance Control	clclpm.p
3.1.1	Inventory Detail Maintenance	icldmt.p
3.1.2	Detail Maintenance by Item/Lot	icitlmt.p
3.1.13	Inventory Detail by Lot Inquiry	icloiq03.p
3.2	Inventory Detail by Item Inquiry	icloiq01.p
3.3	Inventory Detail by Site Inquiry	icloiq02.p

Table 1.17
Modified Programs

Menu Number	Description	Program Name
3.4.1	Transfer–Single Item	iclotr02.p
3.4.3	Transfer With Lot/Serial Change	iclotr03.p
3.4.4	Batchload Transfer with Lot/Serial Change	iclotr04.p
3.6.5	Inventory Detail Report	ppptrp08.p
3.6.6	Inventory Detail by Location	iclorp.p
3.21.1	Transactions Detail Inquiry	ictriq.p
3.24	Inventory Control	icicpm.p
17.1	Labor Feedback by Work Order	sfoptr01.p
17.2	Labor Feedback by Employee	sfoptr02.p
17.3	Labor Feedback by Work Center	sfoptr03.p
17.4	Non-Productive Labor Feedback	sfoptr04.p
17.5	Operation Complete Transaction	sfoptr05.p
17.6	Operation Move Transaction	sfoptr06.p
17.9	Operation Transaction Detail Inquiry	sfopiq12.p
17.14	Operations by Work Order Report	sfopr12.p
17.15	Operations By Employee Report	sfopr13.p
19.11	Quality Order Results Entry	qcwoisrc.p
19.12	Quality Order Results Report	qcpfrp.p
19.13	Test Results Maintenance	mptrmt.p
19.20	Certificate of Analysis Print	mpcarp01.p
36.17.6	Control Table Report	mgpmrp.p

Conversion

Adding Electronic Signatures does not require conversion of existing records. However, new QAD-provided setup data must be loaded.

Minor Enhancements

This section describes minor changes to features of MFG/PRO included in this release. These changes affect the user interface or otherwise alter existing application features. To ensure complete and up-to-date information on minor updates, listings of changes associated with each Engineering Change Order (ECO) in a release are available at the QAD Web site. To view ECO listings, use the following address:

<http://support.qad.com>

To access the ECO listings, you must have a QAD Web account. To obtain a QAD Web account, click the Accounts link at the top of the page.

Product Change Control

To support the overall improvements to security and accountability offered by MFG/PRO eB2.1, several enhancements have been made in Product Change Control (PCC), the module that lets you control and monitor product changes from inception through implementation.

Using enhanced features of PCC, you can:

- Apply electronic signature controls to the approval, incorporation, and implementation functions.
- When electronic signatures are enabled for PCR/PCO Approval (1.9.6.1), prevent the logged-in user from approving documents for another user.
- Based on the value of a new field in PCC Control (1.9.24), enforce the approval sequence defined in the routing slip.
- Apply field security to most database fields in standard maintenance programs that have corresponding functions in PCR Maintenance (1.9.2.1) or PCO Maintenance (1.9.2.13).
- Ensure the completeness of history records by no longer allowing PCR/PCO Delete/Archive (1.9.15) to delete records unless they have been archived.

Global Tax Management Reporting

This release supports new features for Global Tax Management (GTM) reporting.

Taxable and Non-Taxable Amounts

In many taxable documents, a summary of taxable and non-taxable amounts displays on the document trailer. Understanding these summary figures can be confusing when multiple taxes exist for transaction lines and when two taxes have a different tax base. For this reason, you may want to suppress the display of these totals, especially on printed documents received by customers.

The new Display Taxable/Non-Taxable on Trailer field in Global Tax Management Control (2.13.24) determines whether summary totals are included in the order trailer frame in maintenance programs and printed documents.

This field affects the display of taxable amounts in the following programs:

- Sales Order Maintenance (7.1.1)
- Sales Order Print (7.1.3)
- Pre-Shipper/Shipper Confirm (7.9.5)
- Sales Order Shipments (7.9.15)
- Sales Quote Maintenance (7.12.1)
- Sales Quote Print (7.12.3)
- Pending Invoice Maintenance (7.13.1)
- Pending Invoice Register (7.13.2)
- Invoice Print (7.13.3)
- Invoice Post (7.13.4)
- Invoice History Report (7.13.8)
- Closed Invoice Reprint (7.13.12)
- Call Invoice Recording (11.1.1.15)
- Contract Quote Print (11.5.1.3)
- Contract Print (11.5.13.4)

- Contract Invoice Reprint (11.5.18.15)
- RMA Maintenance (11.7.1.1)
- RMA Receipts (11.7.1.13)
- RMA Shipments (11.7.1.16)
- DR/CR Memo Print (27.15)

Additionally, you can use the new Display Taxable/Non-Taxable Total Amounts field in Tax Detail by Transaction Report (2.13.15.3) to determine the report output. When this field is No, these amounts do not display; when Yes, the total amounts display for each reference.

Recoverable and Non-Recoverable Taxes

A new Display Recoverable/Non-Recoverable option has been added to the following reports:

- AP Tax by Transaction Report (2.13.15.16)
- AP Tax by Tax Rate Report (2.13.15.17)

Depending on the setting of this field, the reports display a new column for recoverable or non-recoverable taxes, calculated based on the Percent Recoverable value specified in Tax Rate Maintenance.

Previously, recoverable and non-recoverable amounts could not be reported separately.

Purchasing Taxes

You can use a new purchasing control field to include PST and GST tax IDs on printed purchase orders. When Print Tax ID – Misc on PO is Yes in Purchasing Control (5.24), Purchase Order Print (5.10) includes the PST and GST tax IDs specified in Company Address Maintenance (2.12) in the order header.

Sales and Use Tax Interface

A new Use Sold-To for Tax Usage Exceptions field has been added to Tax Interface Control (36.5.3.24).

When this field is Yes, tax usage codes that display during processing of sales orders, invoices, calls, and return material authorizations (RMAs) default from settings associated with the sold-to customer, rather than the ship-to address. These values are passed to the Vertex application and used in tax calculations.

This feature is useful in situations where the tax exemption status of the sold-to and ship-to addresses is not the same; for example, when items purchased by a non-exempt company are drop-shipped to a non-profit agency.

General Ledger

MFG/PRO eB2.1 includes the following updates to GL functions:

- A Show Non-Selected Transactions field has been added to Account Balance Detail (25.15.2). This lets you control whether the report should be limited specifically to the selection criteria or include transactions that would ordinarily be excluded by such factors as a limited range of daybooks. Previously, the program sometimes produced inconsistent totals when you compared the results with Account Balance Summary (25.15.1).
- In Default Daybook Maintenance (25.8.4), several additional document types can now be associated with inventory control transactions in default daybooks:
 - CN-ADJ: Consignment Inventory Adjustment
 - CN-CNT: Consignment Inventory Count
 - CN-ISS: Consignment Inventory Issue
 - CN-ISSTR: Consignment Inventory Transfer (Issue)
 - CN-RCT: Consignment Inventory Receipt
 - CN-RCTTR: Consignment Inventory Transfer (Receipt)
 - CN-SHIP: Consignment Inventory Transfer (Customer)
 - CN-USE: Consignment Inventory Usage

- MATL-VAR: Material Variance
- FLR-STK: Floor Stock
- MIX-VAR: Mix Variance

Fixed Assets Reporting

Transferred Assets

The Depreciation Expense Report (32.5.7) now correctly presents information about an asset that was transferred between entities within a period included in the report selection criteria. You can use the new Print Transfer Detail field to determine whether information about the transfer is included on the report.

The way the system handles the transfer of suspended assets has been improved. You can now use Fixed Asset Transaction Post (32.13) to create the proper GL transactions when a suspended asset is transferred to another location within an entity or to another entity. New messages display in Fixed Asset Maintenance (32.3). The system displays an error if you try to reinstate a nonsuspended asset. Also the system validates that the reinstatement occurs after any transfer. If not, it issues the following message:

Asset transferred and posted in period N. Reinstate in a later period.

Acquisition Cost

The system now gives you greater control over how you manage the creation of GL transactions for the acquisition cost of an item. After you add a new asset in Fixed Asset Maintenance (32.3) or use the Create function in Fixed Asset Batch Maintenance (32.7), a new frame displays with four fields. The first field is Post to GL. If you respond No, GL transactions for the acquisition cost are not created. Since you may have already accounted for the acquisition cost previously—for example, during purchase order receipt—this prevents double booking of the cost.

If you respond Yes to create GL transactions, you can then specify a GL effective date for the transaction and a daybook to use. Finally you can specify whether to print an audit trail of the GL transactions. If you respond Yes to Print GL Audit Trail, you are prompted for an output device.

Fixed Asset Transaction Post (32.13) no longer creates transactions for the acquisition cost when the first depreciation entry is posted since this transaction, if needed, was created previously when the asset was added. Since these transactions are not created in the post program, you cannot use Fixed Asset Transaction Void (32.14) to void them.

Note The setting of Summarized Journal in Fixed Asset Control (32.24) has no effect on transactions created for acquisition cost. These are always created in detail.

AR Self-Billing Enhancement

A new field has been added to Customer Maintenance (2.1.1) and Scheduled Order Maintenance (7.3.13) that lets you specify how invoice totals should be calculated and displayed: by line or by authorization number.

This field is important for users of the AR Self-Billing module, since customers often submit payment based on authorization numbers. Before this field was introduced, MFG/PRO always calculated totals by invoice line. This could result in rounding discrepancies that made it difficult to close out payments.

Purchasing

Purchasing-related updates include the following:

- A Supplier Lot field has been added to three programs in the Purchasing module.
 - PO Container Maintenance (5.5.5.4, 5.13.13)
 - PO Shipper Maintenance (5.5.5.5, 5.13.14)
 - PO Fiscal Receiving (5.13.16)

The addition of the new field makes these programs consistent with Purchase Order Receipts (5.13.1) for MFG/PRO users who want to associate supplier-assigned lot numbers with purchase order receiving activities.

- In Global Requisition System, GRS Control (5.2.1.24) has been enhanced with two new control options that let you:
 - Prohibit or allow modification of a requisition after the requisition is routed for review and at least one approver has approved it.
 - Reset all approvals after one approver denies the requisition and reroutes the denied requisition back to the originator.

Intrastat History Records

MFG/PRO eB2.1 includes significant changes to how Intrastat records are managed and generated, for both purchasing and sales-related transactions.

Sales-Related Intrastat Records

Prior to these changes, Intrastat history data for sales transactions was collected during invoice post. This could result in legal non-compliance during Intrastat reporting if a time gap existed between shipment of goods and posting the corresponding invoice. It also created problems when the Customer Consignment Inventory module was being used, since only inventory consumed at the customer site was reported on Intrastat declarations, not the inventory that was actually shipped.

The changes to Intrastat include the following:

- Intrastat history data is now collected at time of shipment using the type 1 (shipment) history record. A new type 9 (invoice) record is created during invoice post.
- A new field has been added to Intrastat Control to manage sales-related Intrastat history. The new field is similar to the current Reference Date Logic field, which affects purchasing transactions only. The existing Reference Date Logic field has been renamed PO Reference Date Logic and the new field is SO Reference Date Logic.

Tip

For standard sales orders, only one type of Intrastat history record exists at a time for any sales order line.

- When unreported Intrastat shipment history records exist for a standard sales order, posting an invoice:
 - Changes the Intrastat history record type from 1, indicating a shipment, to 9, indicating an invoice. This effectively deletes the shipment record.
 - Updates the invoice number and invoice date fields in the history record.
 - When SO Reference Date Logic is 2 in Intrastat Control, also updates the reference date with the invoice date.
- The system manages Intrastat history for consigned shipments differently, since customers are invoiced only for the portion of a shipment they have used. In this case, both shipment and invoice type history records can exist simultaneously until all inventory is consumed. Invoice Post updates any unreported shipment data for consigned inventory as follows:
 - Reduces the quantity shipped by the quantity invoiced, and recalculates the invoice value, statistical value, net weight, and supplementary units.
 - When SO Reference Date Logic is 2 in Intrastat Control, updates the reference date, invoice number, and invoice date.
 - When the quantity on the shipment record is reduced to zero, deletes the record. Any future Intrastat reporting is done on the record created by invoicing.
- Declaration Print now checks the value of SO Reference Date Logic in Intrastat Control. If this is 2, any history records without an invoice number are skipped.

Purchasing-Related Intrastat Records

Prior to these changes, Intrastat history data for purchasing transactions was collected only at two points:

- During receipt of goods (type 2 records)
- When the associated receiver was fully vouchered (updated the type 2 records with the invoice cost from the last voucher)

A printed declaration could include erroneous cost information when a receipt was partially vouchered and the purchase order cost differed from the invoice cost of any vouchered quantities. Even when the declaration included information about receivers that were fully vouchered, the statistical value was based only on the invoice cost of the last voucher and did not account for any previous partial vouchers.

To prevent these problems, the following changes were made:

- Intrastat history data is now collected for each vouchered quantity of a receiver at the invoice cost during vouchering using type 6, voucher, records. Previously only type 2 records were created.
- If the received quantity has not been reported already on an Intrastat declaration when vouchering occurs, the quantity received is reduced by the quantity vouchered, and the invoice value, statistical value, net weight, and supplementary units are recalculated. When the quantity on the receipt record is reduced to zero, the record is deleted and reporting is done on the record created by vouchering.
- The label of the Reference Date Logic field in Intrastat Control has been changed to PO Reference Date Logic to distinguish it from the new SO Reference Date Logic field. Having two fields lets the collection of inbound and outbound Intrastat records operate under different rules.

When a voucher is modified or deleted after it has been reported, you must correct the Intrastat history manually using Intrastat Maintenance (2.22.13). If a voucher is deleted before it has been reported, the system updates the receiver's Intrastat history record appropriately.

When the total vouchered quantity for a receipt exceeds the receipt quantity, the system does not collect any more Intrastat data. This is true even when the receipt history has not been reported. When this situation occurs, you should modify the quantity on one of the associated vouchers or correct the Intrastat history manually using Intrastat Maintenance.

Viewing Intrastat History by Order

Use any of the following inquiries to view Intrastat information:

- Intrastat Inquiry by Invoice (2.22.15)
- Intrastat Inquiry by Voucher (2.22.16)

- Intrastat Inquiry by Order (2.22.17)

You can specify new order types using Intrastat Inquiry by Order (2.22.17). Previously, all sales-related history could be viewed by entering SO (type 1). Now sales history created by shipments (type 1) is distinguished from sales history created during invoicing (type 9).

Previously, all purchasing-related history could be viewed by entering PO (type 2). Now, purchasing history created during receipt (type 2) is distinguished from purchasing history created during vouchering (type 6).

You can also use type 3, correction, to view history records created with Intrastat Maintenance (2.22.13).

Conversion

This update requires a one-time conversion of existing sales-related Intrastat history records. After installing this release, use Intrastat SO Invoice Conversion (2.22.25.1) to convert your records appropriately.

Service/Support Management

MFG/PRO eB2.1 includes several enhancements to SSM:

- In Contract Deferred Income Report (11.5.13.21.2), you can now limit the scope of the report by specifying a currency code. When you do this, the report displays the transactions in that currency. Previously, the report included all transactions meeting the selection criteria regardless of the associated currency and displayed them in base currency.
- A field has been added to Call Generator (11.1.8) to let you override the Credit Hold Status setting in Service Management Control when you generate calls for field notifications. When Input Source is F and you set the new Use Credit Hold Option field to No, the system creates calls without checking the credit hold status of the customer. When it is Yes, the system checks the credit hold status and uses the Service Management Control setting to determine processing for customers on credit hold:
 - 0: Generates the call with no credit restriction

- 1: Displays a warning message and generates a call with the status specified in the Hold Status field in Call Management Control
- 2: Displays an error message and does not generate a call

For example, setting the new field to No lets a medical equipment manufacturer generate field notification calls for all customers—regardless of credit status—related to vital equipment repairs.

- Call Activity Recording (11.1.1.13) has been modified to prevent material order lines from becoming stranded when being consumed by call lines.

When the engineer associated with the call line is not the same as the MO-line engineer, the system displays a warning message when the MO line is applied to the call line. Previously, if you pressed End when this message displayed, the MO was neither consumed by the call line nor available for consumption by other lines.

Now, pressing End at the message display makes the MO line available for consumption. As before, pressing Go, Enter, or the spacebar still consumes the MO line on the current call line.

The utility program `utcarmos.p` has been added to update MO line records left stranded before this change was made.

- Installed Base Item Maintenance (11.3.1) now updates the last preventive maintenance (PM) date when you close a non-PM call that includes a PM line. Previously, the system did not update the Last PM Date field under those circumstances.

► See “System Utilities” on page 50.

Trade Management

The Advanced Pricing Management (APM) product has been renamed Trade Management (TrM). All occurrences of APM have been modified accordingly in MFG/PRO menus, messages, field labels, and online help. For example, Sales Order Control (7.1.24) now includes a field labeled Integrate with TrM.

System Utilities

This release adds the following new utilities:

- Delete Stranded Browse Records (36.25.19, `utqadbrd.p`) generates a report by user ID and optionally deletes stranded QAD Workfile (`qad_wkfl`) records.

Various programs—browses, for example—use QAD Workfile to store information temporarily. Ordinarily, these records are deleted by the program that generated them when they are no longer needed. However, terminating the program abnormally can leave stranded `qad_wkfl` records.

When running certain browses, having too many stranded records for a user can impact system performance. Previously, there was no menu option for deleting such records. The new utility addresses that issue.

◆ See “Service/Support Management” on page 48.

- Update Call Act. Rec. Load (36.25.74, `utcarmos.p`) updates the material order detail records on existing stranded MO lines to make them available for consumption in Call Activity Recording.

Continuing MRP/DRP Performance Improvements

MFG/PRO eB2 featured enhancements that let you use a Progress Application Server, or AppServer, to run multithreaded MRP and DRP sessions, resulting in dramatically improved MRP/DRP performance.

MFG/PRO eB2.1 includes a second phase of enhancements that result in better MRP/DRP performance for both Progress and Oracle database configurations that use an AppServer.

Oracle Version

◆ See “Updated Oracle Properties” on page 52 for an updated file example.

To take full advantage of the AppServer performance improvements with an Oracle database, you should be running Oracle version 9.1D05, which corrects a number of problems in version 9.1D. If you are using an earlier version of Oracle with an AppServer, you must add the following parameters to the `ubroker.properties` file:

```
minSrvrInstance=0
autoTrimTimeout=1
```

Documentation Updates

This section identifies changes to the information in *MFG/PRO eB2 User Guide Volume 9: Manager Functions*, Chapter 11, “Application Server.”

Additional Oracle Environment Variables

Add two more environment variables to the entry described under step 1 on page 173:

```
NLS_LANG=AMERICAN_AMERICA.WE8ISO8859P1
NLS_NUMERIC_CHARACTERS=.,
```

Note The NLS variables shown are for American English. Be sure to use appropriate values for your language environment.

Additions to Server Startup Parameters

Update the server startup parameters entry in the `ubroker.properties` file to add references to the parameters file (`.pf`) used at MFG/PRO startup. For Oracle, the startup parameters entry must also include a reference to the unified broker.

Progress example:

```
svrStartupParam=-c 30 -znotrim -d mdy -yy 1920 -Bt 350 -D 100
-mmax 3000
-nb 200 -s 63 -noshvarfix -pf /dr05/mfgpro/eb2/Production.pf
```

Oracle example:

```
svrStartupParam=-Dsrv svub,1 -c 30 -znotrim -d mdy -yy 1920 -Bt
350 -D 100
-mmax 3000 -nb 200 -s 63 -noshvarfix -pf /dr05/mfgpro/eb2/
Production.pf
```

Updated Progress Properties

The following shows the Progress `ubroker.properties` example from user guide page 171 with the updates described in this section in bold text:

```
[UBroker.AS.mt-mrppro]
appserviceNameList=mt-mrppro
brokerLogFile=$WRKDIR/mt-mrppro.broker.log
controllingNameServer=NS1
initialSrvrInstance=12
maxSrvrInstance=20
minSrvrInstance=12
portNumber=50000
PROPATH=/dr05/mfgpro/pro/eb2:/dr05/mfgpro/pro/eb2/us/bbi:
  ${PROPATH}${WRKDIR}
srvrConnectProc=pxldgbl.p
srvrLogFile=$WRKDIR/mt-mrppro.server.log
srvrMaxPort=50202
srvrMinPort=50002
srvrStartupParam=-c 30 -znotrim -d mdy -yy 1920 -Bt 350 -D 100 -mmax 3000
-nb 200 -s 63 -noshvarfix -pf /dr05/mfgpro/eb2/Production.pf
uuid=fdf73fbf039907:6ce891fc:ec7f530e95:-7eed
```

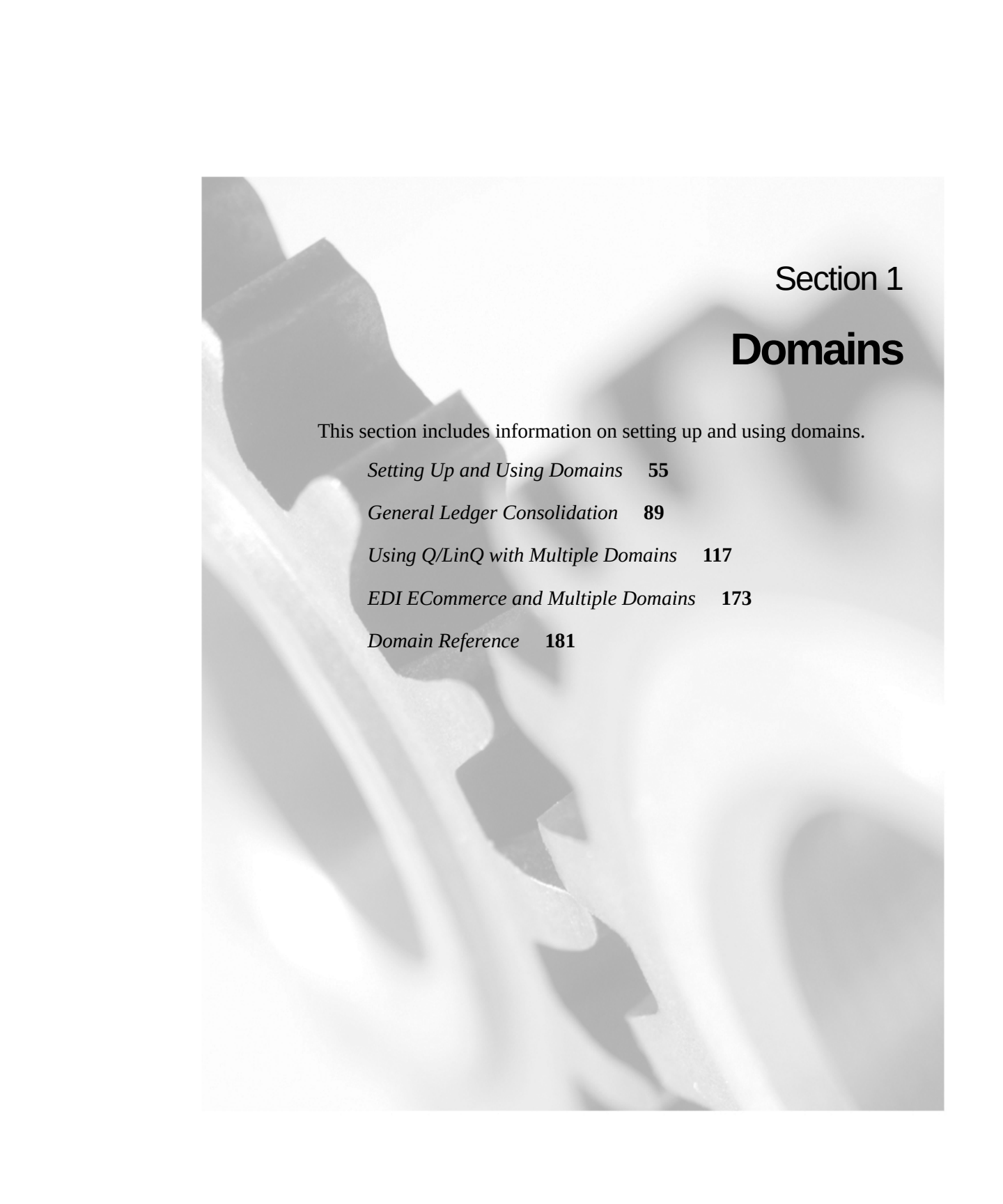
Updated Oracle Properties

The following shows the Oracle `ubroker.properties` example from user guide page 172 with the updates described in this section in bold text:

```
[Environment.mt-mrpora]
ORACLE_BASE=/dr02/apps/oracle/
ORACLE_HOME=/dr02/apps/oracle/8.1.7
ORACLE_SID=mrp
NLS_LANG=AMERICAN_AMERICA.WE8ISO8859P1
NLS_NUMERIC_CHARACTERS=.,

[UBroker.AS.mt-mrpora]
appserviceNameList=mt-mrpora
brokerLogFile=$WRKDIR/mt-mrpora.broker.log
controllingNameServer=NS1
environment=mt-mrpora
initialSrvrInstance=12
maxSrvrInstance=20
portNumber=54000
PROPATH=.:/dr05/mfgpro/eb2:/dr05/mfgpro/eb2/us/bbi:${PROPATH}:${WRKDIR}
srvrConnectProc=pxldgbl.p
srvrLogFile=$WRKDIR/mt-mrpora.server.log
srvrMaxPort=54202
srvrMinPort=54002
minSrvrInstance=0
autoTrimTimeout=1
srvrStartupParam=-Dsrv svub,1 -c 30 -znotrim -d mdy -yy 1920 -Bt 350 -D 100
-mmax 3000 -nb 200 -s 63 -noshvarfix -pf /dr05/mfgpro/eb2/Production.pf
uuid=59fdf73fbf039907:6302bfc1:ec513ed2fd:-6fd7
```

Required only for
Oracle versions earlier
than 9.1D05



Section 1

Domains

This section includes information on setting up and using domains.

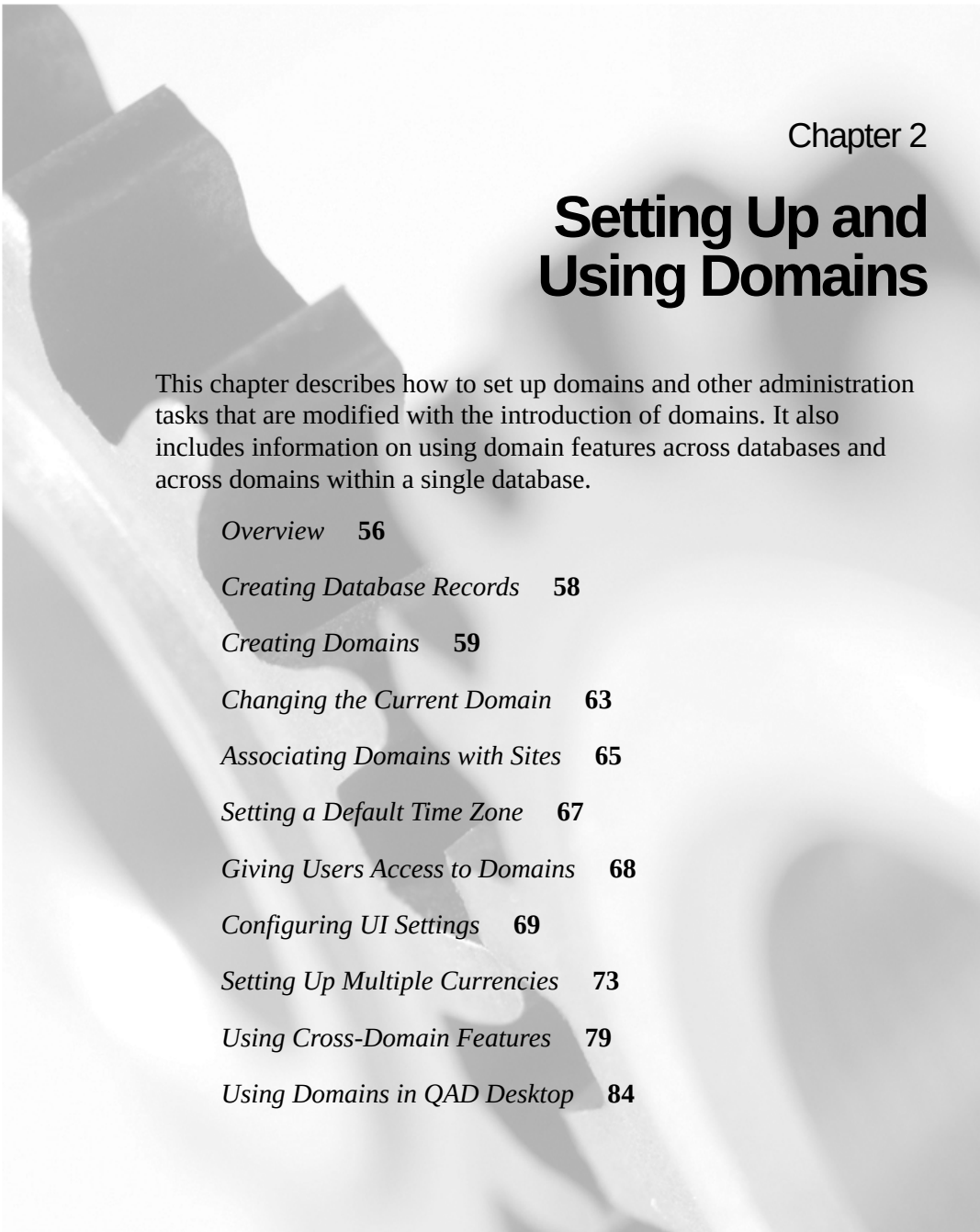
Setting Up and Using Domains **55**

General Ledger Consolidation **89**

Using Q/LinQ with Multiple Domains **117**

EDI ECommerce and Multiple Domains **173**

Domain Reference **181**



Chapter 2

Setting Up and Using Domains

This chapter describes how to set up domains and other administration tasks that are modified with the introduction of domains. It also includes information on using domain features across databases and across domains within a single database.

<i>Overview</i>	56
<i>Creating Database Records</i>	58
<i>Creating Domains</i>	59
<i>Changing the Current Domain</i>	63
<i>Associating Domains with Sites</i>	65
<i>Setting a Default Time Zone</i>	67
<i>Giving Users Access to Domains</i>	68
<i>Configuring UI Settings</i>	69
<i>Setting Up Multiple Currencies</i>	73
<i>Using Cross-Domain Features</i>	79
<i>Using Domains in QAD Desktop</i>	84

Overview

As part of any initial MFG/PRO implementation, you must perform a number of setup tasks including the following:

- Setting up system-wide data such as printers, menus, messages, and language codes
- Defining users and security
- Setting up financial data such as your chart of accounts and entities
- Defining master data such as items, sites, customers and suppliers

Beginning with MFG/PRO eB2.1, you must also complete tasks related to setting up domains. In addition, some previous setup tasks have changed because of changes introduced with domains.

Note Shared Services Domain is a separately licensed MFG/PRO module. Unless you purchase appropriate licences, the system prevents you from having more than one active domain per database.

This chapter highlights setup activities related to or substantially changed by domains.

Implementing Domains

Table 6.1, “Non-Domained Tables,” on page 182 lists the tables in the MFG/PRO database that contain data that applies to the entire database. Data in all other tables is specific to a particular domain. You should consider the implications for data setup carefully during implementation to ensure that users who can change domains do not encounter validation errors.

Generalized Codes Example

Generalized codes are domain specific. This is because when domains represent businesses in diverse geographical and political locations, these codes may vary widely. For example, customer types, sales distribution channels, and buyer/planner codes could differ between a domain representing a business in England and one in Germany.

However, some programs that update system-wide data such as User Maintenance (36.3.1) also reference generalized codes. These generalized codes must exist in all domains or you may encounter errors editing a user record in one domain that do not occur in another.

Streamlining Setup

If you have several domains with similar base data, you can use alternate approaches to streamlining data setup:

- You can set up base data in the system domain. When you create a new domain, the system domain is used as a template and the new domain automatically inherits the same system data.
- You can use the synchronization features of Q/LinQ to replicate data from selected tables across domains.

▶ See “System Domain” on page 59.

▶ See Chapter 4, “Using Q/LinQ with Multiple Domains,” on page 117.

Domain Setup Work Flow

Figure 2.1 illustrates the steps required to set up domains in a database.

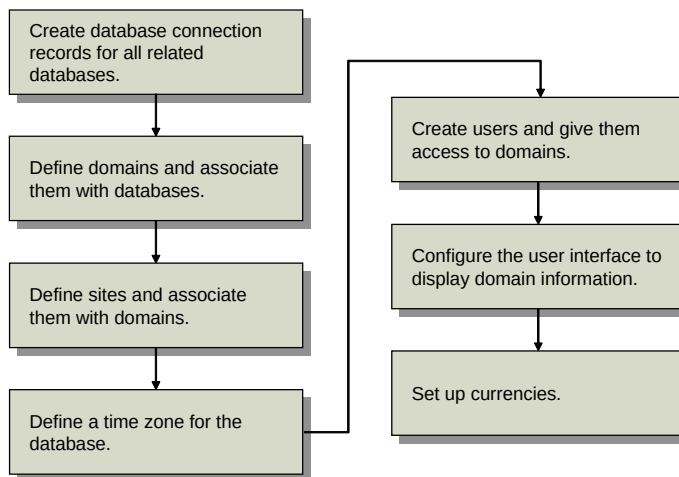


Fig. 2.1
Domain Setup
Work Flow

- ♦ See page 58.

1 Identify each database in Database Connection Maintenance (36.6.1) and define its location and connection parameters. You must create a record for the working database even when you are not using multiple databases.
- ♦ See page 59.

2 Create domains in Domain Maintenance (36.10.1) and associate them with databases. Domain names should be unique across connected databases.
- ♦ See page 65.

3 Assign each site to the appropriate domain in Site Maintenance (1.1.13).
- ♦ See page 67.

4 Define a time zone for the database in Database Control (36.24).
- ♦ See page 68.

5 Create users and give them access to domains in User Maintenance (36.3.1).
- ♦ See page 69.

6 Configure settings that affect the display of domain information on the user interface using Security Control (36.24) and Program Information Maintenance (36.3.21.1).
- ♦ See page 73.

7 Set up currency codes for use with multiple domains using a number of programs on the Multiple Currency Menu (26).

Creating Database Records

In a multiple-database environment, use Database Connection Maintenance (36.6.1) to specify the MFG/PRO databases on your network and how to connect to them.

For a single database, you must still create a connection record that defines the database name. Only databases defined in this program can be associated with domains in Domain Maintenance.

Note A record for qaddb is automatically loaded with the system data during installation.



Fig. 2.2
Database
Connection
Maintenance
(36.6.1)

Creating Domains

Use Domain Maintenance (36.10.1) to define domains in the current database. You create two types of domains:

- *Primary* domains reference the current database.
- *Connection* domains point to domains located in other databases.

Most MFG/PRO functions update data within a specific domain. For example, each domain has its own base currency, chart of accounts, and control settings. All business documents—such as sales orders, purchase orders, and work orders—reference a specific domain.

A few system maintenance functions update data shared by all domains. These include functions such as printers, users, menus, messages, and currency codes.

The Header Display Mode setting in Security Control (36.3.24) determines if the current domain name displays in program title bars in the character and Windows user interfaces. When the domain name displays, programs that update shared data display All Domains in the title bar. Programs that update domain-specific data display the domain short name and currency instead.

◆ Table 6.2 on page 185 lists these functions.

◆ See “Setting Display Mode” on page 69.

System Domain

Every database must have one system domain, indicated by a domain type of SYSTEM. The initial system domain is created when the database is created, for both a new installation of MFG/PRO or a conversion. The

initial system domain code is QAD. You can change the domain name and short name—but not the domain code—using Domain Maintenance as needed.

◆ See Table 6.3, “Tables Copied for New Domain,” on page 188.

The system domain includes default data that is required to begin implementing MFG/PRO, such as control program settings, rounding methods, default accounts, and generalized codes.

The system domain is used as a template for new domains. When you create a new domain associated with the current database, default data is copied from the system domain. This default data is not added to connection records, which reference another database that contains the actual data associated with a domain.

Since the system domain is used as a template, you may want to add data to it or tailor defaults before creating new domains based on it.

◆ See “Giving Users Access to Domains” on page 68.

The system domain is typically not used for maintaining active transactions. You can prevent users from updating it by setting its Active field to No and by restricting access in User Maintenance (36.3.1).

Multiple Database Validations

When you create a domain, you must associate it with a database. When you create a new primary domain (database is your current database) in a multi-database environment, all databases must be connected. The system verifies that the domain you are about to create does not already exist as a primary domain in another connected database. If it does, an error displays and you cannot continue.

◆ See “Site Connection Records” on page 65.

If the database you specify is not the database you are currently logged in to, the domain is considered a connection record. Normally, you do not need to create connection records manually. When you create a new primary domain, the system automatically creates connection records in other databases defined in Database Connection Maintenance (36.6.1).

If you do create a connection record manually, the system verifies that the domain exists as a primary domain in a connected database. Otherwise, an error is generated.

When you are using multiple databases operating over a network, the system uses the domain associated with a site to determine where database records should be updated.

Active and Inactive Domains

To ensure data integrity, you cannot delete a domain. Instead, set the Active field to No. This prevents users from specifying this domain at log-in or using Change Current Domain (36.10.13) to switch to it later.

Note Unless you have a license for Shared Services Domain, only one domain can be active at the same time.

In a multiple-database environment, you can only change the active status of domains in the current database, and then only when all other databases are active and connected. The system modifies the Active field for the connection records that exist in the other databases. An error displays if any database cannot be accessed and you cannot change the active status.

Domain Maintenance

Figure 2.3 illustrates Domain Maintenance (36.10.1).

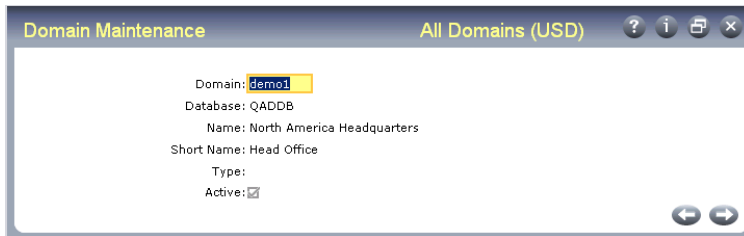


Fig. 2.3
Domain
Maintenance
(36.10.1)

Domain Code. Enter a code (up to 8 characters) identifying a specific domain. Codes are restricted to the characters A–Z, a–z, and 0–9.

Domain Name. Enter a descriptive name to associate with this domain (up to 28 characters). This name must be unique within a database and across connected databases.

This name displays in the lookup associated with domain fields and on various reports and inquiries, as space permits.

Note When you change the domain name, the system automatically sets the value of ~SCREENS and ~REPORTS to the new domain name. You define these values in Company Address Maintenance (2.12) to represent your company name on the top of menus and reports.

◆ See “Setting Display Mode” on page 69.

Domain Short Name. Enter a brief name (up to 14 characters) to associate with this domain. This name must be unique within a database and across connected databases.

The domain short name displays in the program title bar in the character and Windows interfaces based on the setting of Header Display Mode in Security Control. It always displays in the program title in Desktop screens.

Database. For a new domain, enter the name of the database where the domain is located. Set up databases in Database Connection Maintenance (36.6.1). You must specify a database even in a single-database environment. This is to ensure proper setup data exists if you decide to add other databases later.

Once a domain exists, this field cannot be edited. Database defaults to your current working database.

Domain Type. Enter a code identifying the type of domain. You can use this field to group domains based on a user-defined convention.

◆ See “System Domain” on page 59.

One domain in each database must be defined with a domain type of SYSTEM, which is used as a template for supplying default data when other domains are created.

You cannot modify the type of the system domain. However, you can change another domain to be the system domain by modifying its type to SYSTEM. In this case, you are prompted to continue. If you respond Yes, the type of the current system domain is set to blank and the domain you are editing becomes the system domain.

Note A connection record cannot have a type of SYSTEM.

Active. Indicate whether this primary domain is currently active.

Yes (the default): This domain can be associated with users in User Maintenance and specified at log-in.

No: This domain is not active in the current database.

Note Unless you have purchased the Shared Services Domain module, the system lets you have only one active domain. If you attempt to activate a domain when your database already has an active domain, an error message displays.

When new sites are created in Site Maintenance (1.1.13), a site connection record is created in active domains only.

The system performs the following validations related to this field:

- You cannot change the Active setting of your current domain. You must switch domains first and then modify the other domain to inactive.
- You cannot change this field if the domain is a connection record (referencing another database). You must change this field in the domain's primary database.
- In a multiple-database environment, you can only change this field for a domain in the current database when all other databases are active and connected. The system modifies the Active field for the connection records that exist in the other databases. An error displays if any database cannot be accessed and the field cannot be changed.

♦ See “Associating Domains with Sites” on page 65.

Viewing Domain Information

Use either of the following two functions to view information about domains:

- Domain Browse (36.10.2)
- Domain Report (36.10.3)

Changing the Current Domain

You can use Change Current Domain (36.10.13) to change the active domain in your current session to another domain associated with your ID in User Maintenance (36.3.1).

Figure 2.4 illustrates Change Current Domain.

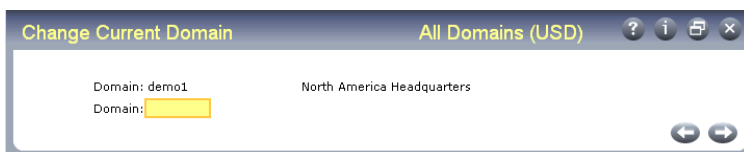


Fig. 2.4
Change Current
Domain (36.10.13)

Note If only one domain is assigned to you, an error displays when you attempt to execute this program.

This function is useful for system administrators, corporate controllers, or others with system-wide responsibility who regularly access and update information in multiple domains.

This function affects your current session only. Each time you log in, you are prompted to specify a domain. The domain designated as default in User Maintenance displays by default.

When you change domains, the system accesses information about the new domain such as the base currency and primary entity.

♦ See “Using Domains in QAD Desktop” on page 84.

Note Changing domains does not affect the domain associated with detached windows in QAD Desktop.

Domain Access

You can only change to an active domain you have been given access to in User Maintenance. If you are assigned to a different user group in the new domain, the functions you can perform may be different from the functions you performed in the previous domain.

Database Switching

If you change to a domain associated with a database other than the current one, database switching is initiated. The system connects to the database using the information set up in Database Connection Maintenance. If the connection cannot be made, a message displays.

This is equivalent to logging out of MFG/PRO and starting a new MFG/PRO session in a different database.

Note When you switch databases using this program, the system checks your security access based on the user groups defined for your user ID in the target domain and database.

Associating Domains with Sites

Each site must be associated with a domain. When a site is associated with the current working domain, it is considered a primary site; otherwise, it is a connection record pointing to the domain where the actual site-related data is maintained. The other domain can be in this database or in another connected database.

Figure 2.5 illustrates the Domain field in Site Maintenance (1.1.13).

The screenshot shows a window titled "Site Maintenance" with a subtitle "Head Office (USD)". The window contains several fields for site configuration. A label "Domain field" with a line pointing to the "Domain:" field is positioned to the left of the window. The fields are as follows:

- Site: 21020000
- Description: Los Angeles
- Entity: 1000
- Default Inventory Status: [dropdown]
- Automatic Locations: [checkbox checked]
- Domain: demo1
- EMT Supplier: [dropdown]
- External Supplier: [checkbox]
- Transfer Variance Acct: 5030
- Transfer Ownership: [checkbox]

At the bottom right of the window are three buttons: a red 'X' (close), a left arrow (previous), and a right arrow (next).

Fig. 2.5
Site Maintenance
(1.1.13)

When you are using multiple databases operating over a network, the system uses the domain associated with a site to determine where database records should be updated. For example, when a function such as DRP requests information for a site, the system looks up the database name associated with the domain record and accesses that database automatically. This can be the current database, another database on the same machine, or a remote database on another machine.

Site Connection Records

To help you manage the relationships among sites and domains, you can optionally create connection records in related domains when you create a new primary site.

Note You can also create a connection record directly by specifying a domain other than your current working domain. In this case, the system ensures that the site already exists as a primary site in a different domain, or an error is generated.

Choosing Domains to Update

The system generates a list of active domains in the current database and all databases defined in Database Connection Maintenance. You can choose which domains to update from this list.

Before the list displays, you are prompted to set a default for the Update field. Set this to Yes if you want to create connection site records in most related domains. You can then change exceptions to No.

Fig. 2.6
Creating
Connection
Records in Site
Maintenance

Domain	Name	Database	Update
12345678	Domain for Header Display Ct	QADDB	☒
afp	afp domain	QADDB	☐
ahh-1	Abbas's Domain 1	QADDB	☐
ani	Anitha	QADDB	☐
demo2	European Operations Demo2	QADDB	☐
dom1	domain1 for site 1	QADDB	☐
dom2	domain2	QADDB	☐
dsk-dom	DSK Domain	QADDB	☐
epm-dom1	epm domain 1	QADDB	☐
eyk	Elma's domain	QADDB	☐

Note In a multi-database environment, all databases must be connected or you cannot create a new primary site record. This is to ensure that the site does not already exist as a primary site in a domain in another database. This is also true when you delete a primary site, although in this case, additional restrictions may prevent you from deleting the site.

Connection Site Defaults

The data associated with the site connection record defaults from the primary site record but is validated in the target domain:

- The entity associated with the site must exist in the connection domain or an error is generated.
- The connection record is created with the primary site’s default inventory status if the inventory status is valid in the connection domain. Otherwise, the first inventory status in that domain is used.
- The site connection record is created with the same Transfer Clearing account, sub-account, and cost center as the primary site if this combination is valid in the target domain. Otherwise, the value from

Inventory Control (3.24) in the target domain is used. If this is not found, the value from Domain/Account Control (36.1) in the target domain is used.

Deleting Sites

The system performs a number of validations if you attempt to delete a site to ensure that it is not referenced and required by other data and transactions. If a primary site passes all these validations, the system performs additional domain-related validations:

- All connection records must also be able to be deleted.
- In a multiple-database environment, the system checks that all databases are connected before you can delete a primary site record.

If no other restrictions apply to the deletion, the primary site is deleted and all connection records are also deleted from other domains in this and connected databases. The system does not check other domains when you delete a connection record.

Setting a Default Time Zone

The server time zone applies to the entire database. Use Database Control (36.24) to specify the time zone of the database. You should do this before defining users since the time zone specified here defaults when new user records are created.

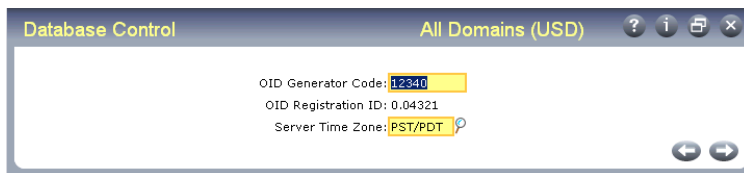


Fig. 2.7
Database Control
(36.24)

Enter the time zone associated with the server machine for the current MFG/PRO database. The system verifies that this is a valid time zone defined in Multiple Time Zones Maintenance (36.16.22.1).

When a new user is created in User Maintenance (36.3.1), the user time zone defaults from the server time zone.

If you are using the optional Service/Support Management module and the Multiple Time Zone option is activated in Service Management Control (11.24) for any domain in the database, this field cannot be modified here. Instead, you must use the Server Time Zone Change Utility (11.21.22.22).

♦ See the installation guide for your system for information.

Note The OID Generator Code in Database Control is used to assign unique object identifiers (OIDs) to database records for auditing purposes. The code is assigned during system implementation.

Giving Users Access to Domains

♦ See “Specifying Domains” on page 231.

Use User Maintenance (36.3.1) to create users and assign each user access to one or more domains. You can:

- Specify one or more domains in the current database that this user can access. Menu functions the user can execute in each domain are determined by the user’s group assignment.
- For users who can execute functions in more than one domain, indicate which domain they normally use. This domain is the default during log-in.
- Assign the user to one or more groups in each domain this user can access. Use groups to streamline security setup for menus, entities, sites, and other functions that allow specification of a user group. This is an optional feature.

♦ See “Controlling Access with User Groups” on page 234.

Note User profiles apply to all domains in the system. However, profiles include several generalized codes that are domain specific such as access location and user type. To prevent validation errors, you should ensure that these codes exist in all domains.

Configuring UI Settings

Domains add a new element to a user's working context. In a multiple-domain environment, users need to know their current working domain and currency, as well as when they are using a program that updates information that applies to all domains.

This section discusses some of the ways you can configure and view domain-related information on the UI:

- You can use settings in Security Control (36.3.24) and Program Information Maintenance (36.3.21.1) to control the information about domains that displays on each screen in MFG/PRO.
- You can view the user's working domain in Session Master Maintenance (36.20.10.15).
- You can review enhanced context information using the Ctrl+F key combination.

Note Some of these settings affect the character and Windows UIs only.

Setting Display Mode

Use the Header Display Mode field in Security Control (36.3.24) to control the information that displays in the menu and program title bars of MFG/PRO programs in the character and Windows user interfaces.

Note Display mode does not affect the display of programs in QAD Desktop. Desktop programs always show the domain short name and currency in the program title bar. To view the user ID, you can click the information (i) icon, which displays details about the program you are running. The user name displays in the browser title bar.

Based on such factors as security requirements, you can choose to display:

- The date only
- The ID of the logged-in user only
- The date and domain name
- The user ID and domain name

◆ See page 215 for details about each display mode.

♦ See “Using Ctrl+F to View Information” on page 71.

When you select an option that includes the domain name, the name of the program currently being executed no longer displays on the UI. In the character and Windows interfaces, you can use the enhanced Ctrl+F key combination to review this information and other context details. In QAD Desktop, click the information icon (i) to display details about the program.

Updating Program Information

Tip
This field affects all MFG/PRO UIs.

You can use a setting in Program Information Maintenance (36.3.21.1) to control which programs display the string All Domains in the title bar.

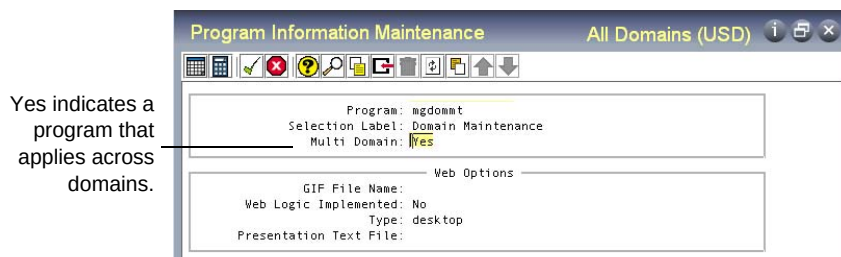
- In the character and Windows interfaces, this displays when Header Display Mode is 2 or 3.
- In Desktop, either the domain name or All Domains displays regardless of the Security Control setting.

♦ See Table 6.2 on page 185 for a list of programs that display All Domains.

Information about all MFG/PRO programs is initially loaded into your database during installation with appropriate default settings. You can update the setting for your custom programs or change it if you want the current working domain to continue to display even when a user is updating a table that applies across domains.

Note This change affects what displays on the UI, only. The program continues to update data for all domains.

Fig. 2.8
Program Information Maintenance (36.3.21.1)



Multi Domain. Indicate if this program updates data that applies to all domains in the database.

No: The data referenced by this program is specific to the current working domain. For example, generalized codes apply to each domain separately so Multi Domain is set to No by default for mgcodemt . p.

Yes: The data referenced by this program is not part of a specific domain. For example, country codes apply to the database as a whole so by default Multi Domain is set to Yes by default for `adctrymt.p`.

When Header Display Mode is 2 or 3 in Security Control and a user invokes a program, the system checks the value of this setting to determine what to display in the program title bar.

- When Multi Domain is No, the short name and base currency of the current working domain display.
- When Multi Domain is Yes, the string All Domains displays in the header to help users easily identify functions that operate across domains.

Tip
Base currency of the working domain continues to display.

Using Ctrl+F to View Information

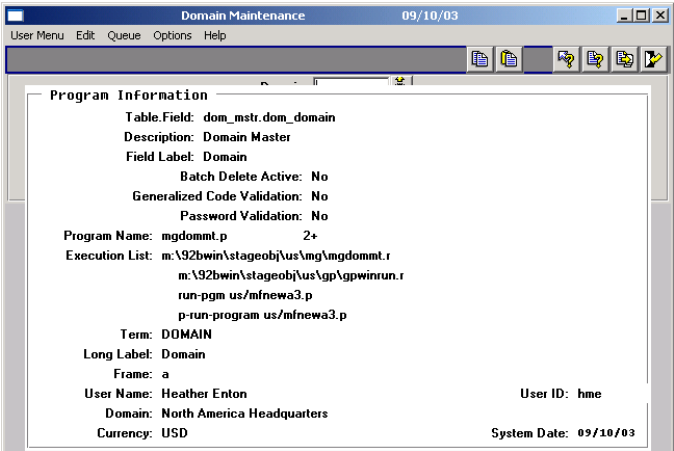
In previous releases of MFG/PRO, the Ctrl+F key combination displayed a message at the bottom of the screen with information about three possible field validations:

- Generalized codes
- Field security
- Batch delete

Tip
Ctrl+F works in character and GUI interfaces only.

Ctrl+F now displays a pop-up window like the one illustrated in Figure 2.9 with more complete information about the context of the current field. This includes the program name being executed, which previously displayed on the title bar in the character UI.

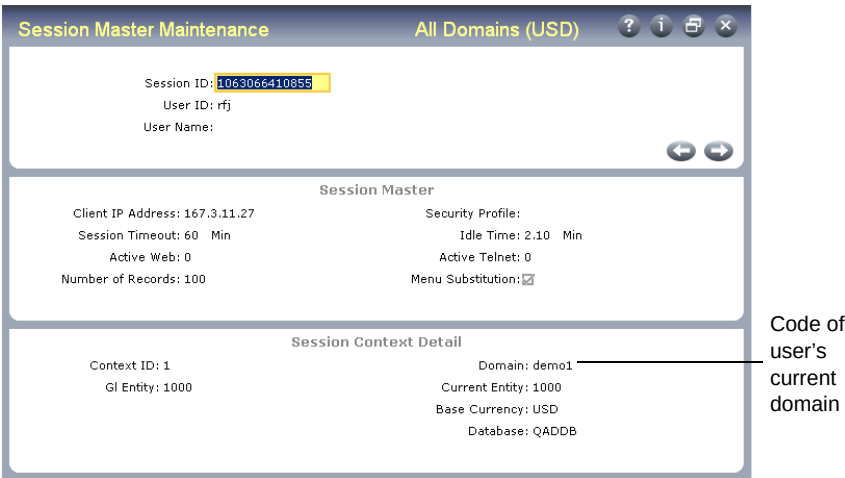
Fig. 2.9
Ctrl+F Pop-Up
Display



Viewing Session Details

You can use Session Master Maintenance (36.20.10.15) to view information about users currently logged in to the system and details about their log-in sessions, including the current working domain.

Fig. 2.10
Session Master
Maintenance
(36.20.10.15)



Setting Up Multiple Currencies

The addition of domains to a database lets you have multiple business operations using different base currencies in one database.

To support this, a number of changes and enhancements have been made to the way you set up currencies and exchange rates. Figure 2.11 illustrates the steps involved in creating currencies for use with multiple domains.

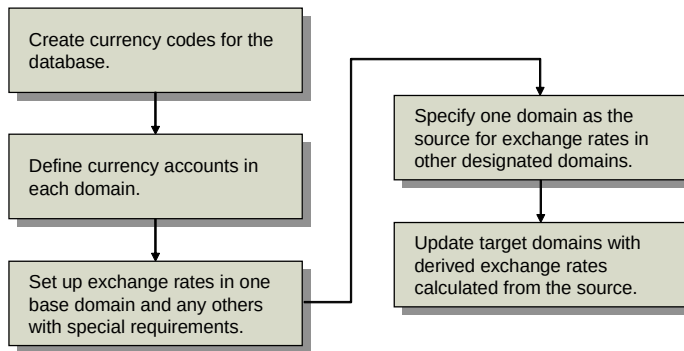


Fig. 2.11
Currency Setup
Work Flow

- 1 Set up currency codes that apply to all domains in Currency Maintenance (26.1).
- 2 Set up currency accounts for each domain in Currency Account Maintenance (26.7). These accounts default from Domain/Account Control, so if the default accounts are acceptable, this step is not required.
- 3 Set up exchange rates in Exchange Rate Maintenance (26.4) in at least one domain. These values apply to the current working domain. If regulatory requirements dictate specific rates in other domains, set up rates in each of these also.
- 4 Use Exchange Rate Relationship Maintenance (26.10) to designate one domain as the source of exchange rate information for other related domains.
- 5 Use Derived Exchange Rate Calculation (26.12) to update the rates in the destination domains.

Defining Currencies

Use Currency Maintenance (26.1) to define the static data associated with a currency in all database domains: description, rounding method, and whether the code is active.

Fig. 2.12
Currency
Maintenance (26.1)

The screenshot shows the 'Currency Maintenance' window for 'All Domains (USD)'. The fields are as follows:

Field	Value
Currency	USD
Description	United States Dollar
Rounding Method	2
Active	☒

Defining Currency Accounts

Since each domain can have its own chart of accounts, the accounts associated with a currency may vary from one domain to another. Use Currency Account Maintenance (26.7) to define the six accounts associated with each currency in the current working domain.

Fig. 2.13
Currency Account
Maintenance (26.7)

The screenshot shows the 'Currency Account Maintenance' window for 'Head Office (USD)'. The table displays the following data:

	Currency: USD	United States Dollar
Unrealized Exchange Gain Acct:	1035	
Unrealized Exchange Loss Acct:	1036	
Realized Exchange Gain Acct:	1037	
Realized Exchange Loss Acct:	1038	
Exchange Rounding Account:	1039	

These accounts default from values previously defined in Domain/Account Control (36.1).

Defining Exchange Rates

Exchange rates apply only to the domain in which they are defined. Set up exchange rates in Exchange Rate Maintenance (26.4). This program has not been changed by features introduced with domains.

Defining a Source Domain

Use Exchange Rate Relationship Maintenance (26.10) to specify a domain as the source of exchange rate information for other related domains.

Use this function to streamline the maintenance of exchange rates in a database with more than one domain when the domains share common rates.

Note In some countries, exchange rates are mandated by government regulation and must be maintained separately.

Figure 2.14 illustrates Exchange Rate Relationship Maintenance.

Fig. 2.14
Exchange Rate
Relationship
Maintenance
(26.10)

Source Domain. Enter a valid, active domain that references the current database. The system verifies that you have access to this domain in User Maintenance. The default is the current operating domain. The domain short name, base currency, and base currency description display.

Only one domain can be designated as the source of exchange rate information. You can access this field only when no relationships are defined. Once you have defined a source and destination relationship, all other relationships use the same source.

To change the source, you must delete all defined relationships.

Destination Domain. Enter a valid, active domain that references the current database. The system verifies that you have access to this domain in User Maintenance. The domain short name, base currency, and base currency description display. Exchange rates can be calculated in the destination domain based on data in the source domain.

Calculating Derived Exchange Rates

Use Derived Exchange Rate Calculation (26.12) to update exchange rates in destination domains for a designated period based on values in a source domain.

▶ See “Defining a Source Domain” on page 75.

Note You must first specify the source domain in Exchange Rate Relationship Maintenance. If no relationships have been defined when you attempt to execute this program, an error displays.

You can execute this function interactively or in batch. When you execute the program interactively, you can choose which domains to update by setting Select Domains to Yes. Otherwise, all domains for which relationships exist are updated. Batch mode always updates all domains related to the source domain.

Correcting Errors

Errors such as the following can occur that prevent exchange rates from being updated in a specific domain:

- You have not been assigned access to the destination domain in User Maintenance.
- An exchange rate between the base currency of the source domain and the base currency of the destination domain does not exist for the entire period specified.

To review possible errors, execute this function in report-only mode. If any errors display, you can correct them. When you are satisfied with the derived exchange rates, set Update to Yes to update the database.

If an error occurs in update mode, you must fix the problem and rerun the program interactively so you that can select the specific domains that were skipped.

Calculations

When the base currency of the destination domain is the same as the source, exchange rates are simply copied. When the base currencies are not the same, the system calculates rates based on information in the source domain.

The system overwrites any rates defined in the destination domain using the following rules:

- If the start date of the existing rate is before the start date of the period being calculated and the end date is in the period, the end date of the existing rate is set to the day before the new exchange rate starts.
- If the start date of the existing period is before the start date of the period being calculated and the end date is after the period, the existing rate is split into one ending the day before the new period and one starting the day after.
- If the start date of the existing period is in the period being calculated and the end date is after the period, the start date of the existing rate is set to the day after the end date of the period being calculated.
- If the start and end dates of the existing period are within the period being calculated, the existing rate is deleted.

The system uses the rates defined in the source domain between currency A and B and between currency A and C to derive the rate between B and C in a destination domain.

For example, Domain 1 has a base currency of EUR and exchange rates as follows:

$$1 \text{ EUR} = 2 \text{ GBP}$$

$$1 \text{ EUR} = 3 \text{ USD}$$

Domain 2 has a base currency of GBP. The derived rate between GBP and USD is:

$$1 \text{ GBP} = 3/2 \text{ USD} = 1.5$$

For Domain 3 with a base currency of USD, the derived rate between USD and GBP is:

$$1 \text{ USD} = 2/3 \text{ GBP} = 0.66 \text{ GBP}$$

A unit of 1 is assumed. If a scaling factor needs to be applied to accommodate large differences in currency value, do this manually in the destination domain.

Figure 2.15 illustrates Derived Exchange Rate Calculation (26.12).

Fig. 2.15
Derived Exchange
Rate Calculation
(26.12)

Derived Ex Rate Calculation All Domains (USD)

Source Domain: demo1 North America Headquarters Base Currency: USD

Start Date: 09/08/2003 End Effective: 09/08/2003

Sel: ☒ Update: ☒ Output: Batch ID:

Start and End Date. Enter the starting and ending dates for the exchange rates to be generated in destination domains.

When the source and destination domains have different base currencies, an exchange rate between the two currencies must exist in the source domain for the entire period specified. Otherwise, the calculation cannot be performed and an error displays.

Select Domains. If you are not executing this program in batch, indicate if you want to manually select domains to be updated.

No: The calculation is performed for all domains with a relationship to the source domain as defined in Exchange Rate Relationship Maintenance.

Yes: A list displays with all domains that are related to the source domain. By default, all domains are selected. You can modify the selection for specific domains as needed.

This field has no effect if you specify a batch ID. In batch mode, all domains with relationships to the source are updated.

Figure 2.16 illustrates the selection list that displays when you calculate exchange rates interactively and set Select Domains to Yes.

Fig. 2.16
Selecting Domains
to Update

Derived Ex Rate Calculation All Domains (USD)

Source Domain: demo1 North America Headquarters Base Currency: USD

Start Date: 09/08/2003 End Effective: 09/08/2003

Sel: ☒ Update: ☐ Output: Batch ID:

Select Domain

Sel	Domain	Name
*	demo2	European Operations Demo2

Using Cross-Domain Features

Some functions in MFG/PRO update data in remote, connected databases. These functions can now also be used to update data in domains within the same database. In addition, a number of functions have been enhanced or added that provide visibility across domains in a database. This section discusses these two types of functions.

Using Multi-Database Functions Across Domains

Previous releases of MFG/PRO included a number of functions that updated data in more than one database. Database switching was automatically initiated when one of the sites referenced in the function existed in a different database. The system determined the database involved based on information defined in Site Maintenance (1.1.13).

With the introduction of domains, these functions can still be used across databases. However, they can also be used across domains within a single database. Using these functions in this context often is more efficient and streamlined.

This section discusses three such functions and points out the differences in how they work across domains rather than across databases.

- Enterprise Material Transfer (EMT)
- Distribution Requirements Planning (DRP)
- Enterprise Operations Planning (EOP)

Using Enterprise Material Transfer

When Use Enterprise Material Transfer is Yes in Sales Order Control (7.1.24), you can create EMT sales orders. EMT automatically translates sales orders into purchase orders. You then transmit them to the appropriate supplier using EDI ECommerce. EMT also manages and coordinates changes so that sales order and purchase order information is synchronized.

Multi-level EMT manages orders across multiple levels within an organization. Order changes can be made at the top or bottom of the hierarchy and are then transmitted up or down to the next level.

♦ See *User Guide Volume 2: Distribution* for details.

With the introduction of domains, EMT can function between business organizations in one domain, in different domains within the same database, or in different MFG/PRO databases. The way EMT functions in these various scenarios is basically the same. However, if the related business units are represented by different domains within the same database, it becomes easier to use the direct allocation feature of EMT.

With direct allocation, the primary business unit (PBU) can make a special, temporary allocation of an EMT sales order or material order line item at the secondary business unit (SBU) site. When the SBU imports the PBU's EMT purchase order to create a secondary sales order, the system automatically converts this temporary allocation to a general allocation.

When the different business units in an EMT relationship are in separate databases, direct allocation can be used only when the business partners use the same version of MFG/PRO and when the databases are connected.

The following list summarizes the scenarios supported for EMT:

- Within a single database where the PBU and SBU are within the same domain.
- Within a single database where the PBU and SBU are in different domains.
- Across multiple databases where the PBU and SBU are in different domains.
- Across multiple databases where the PBU is in a database with domains (eB 2.1 or higher) and the SBU is in an MFG/PRO database on an earlier release. In this case, direct allocation cannot be used.
- Across multiple databases where the PBU is in a database without domains (earlier than eB2.1) and the SBU is in a database with domains (eB2.1 or higher). In this case, direct allocation cannot be used.

Note The SBU could also be using a non-MFG/PRO system. Direct allocation is not supported in this scenario either, regardless of the PBU's MFG/PRO version.

Using Distribution Requirements Planning

In a multiple database environment, you can use DRP to plan supply to meet demand for multiple sites within the current database and distribute demand to other connected databases. DRP can be used only under the following conditions:

- The base currencies of the databases are the same.
- Taxes do not need to be calculated.
- Customs documentation is not needed.

With the introduction of domain, you can now use DRP to plan supply to meet demand for multiple sites within a single domain, and to distribute demand to:

- Other sites within the current domain
- Other sites in other domains within the same database
- Other sites in connected, remote databases

The execution of DRP with domains does not require any special setup. The system determines whether database switching is needed based on the domain associated with the site in Site Maintenance.

If all of your domains are located in one database, the DRP process is simplified since you never have to be concerned about database connections not being available. In this case, the following functions are not needed:

- Intersite Demand Validation (12.17.12), which is run at the supply database to search for all changes to intersite demand that occurred in the demand database while the database connection was not available
- Intersite Demand Transfer (12.15.9), which is used to transfer system-generated intersite requests to the supply site's database
- Intersite Demand Export (12.15.10), which is used to place demand records in an ASCII file to send to the supply site
- Intersite Demand Import (12.17.10), which is used to import demand records in an ASCII file into the supply site's database

◆ See *User Guide Volume 5: Supply Chain Management* for details.

Tip
These are the same restrictions that applied before introduction of Domain.

◆ See “Associating Domains with Sites” on page 65.

Using Enterprise Operations Planning

▶ See *User Guide Volume 5: Supply Chain Management* for details.

Functions in the Enterprise Operations Planning (33) module let you plan for end items and family items for multiple sites both within a single database and across multiple connected databases. With the introduction of domains, you can also execute planning functions for sites in multiple domains within a single database.

▶ See “Associating Domains with Sites” on page 65.

The execution of Enterprise Operations Planning with domains does not require any special setup. The system determines whether database switching is needed based on the domain associated with the site in Site Maintenance.

Using Features Across Domains in a Database

The previous section describes functions that work across databases and domains. This section describes functions that let you view and manage data across domains only. These functions include:

- Two new reports that display transaction numbers across domains
- Functions for managing batch requests

▶ See Chapter 4 and Chapter 5.

Note Cross-domain administrative features have also been added to EDI ECommerce and Q/LinQ. These are documented separately.

Viewing Transaction History Across Domains

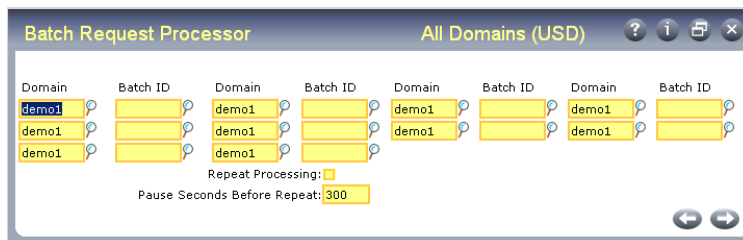
If your database has multiple domains, you can use two new reports to review transaction numbers in sequence. Since sequence numbers apply to the database as a whole, transactions within a domain may appear to have gaps. This report lets you see transactions created in all domains and verify that numbering is sequential.

- Use Transaction Numbering Report (3.21.19) to review inventory transaction history by number or date range.
- Use Operations Numbering Report (17.13.22, 18.4.16, and 18.22.4.12) to review operation transaction history by number or date range.

Submitting Batch Requests

Batch Request Processor (36.14.13) has also been modified to let you specify each domain associated with the 10 batch IDs that can be processed at the same time.

Fig. 2.19
Batch Request
Processor
(36.14.13)



A new Batch Request Browse (36.14.4) lets you quickly review requests that have been submitted for a range of domains. The Batch Request Detail Report (36.14.5) also supports selecting detail by a range of domains.

Using Domains in QAD Desktop

► See “Setting Display Mode” on page 69.

The new features introduced by Domain are essentially the same across all MFG/PRO user interfaces. How the domain name displays on screen titles does vary in the different UIs.

In QAD Desktop, the domain short name and currency always displays on program title bars. The user ID can be seen by clicking the information (i) icon to display the information window.

The QAD Desktop interface supports additional navigation and UI features not available in other MFG/PRO UIs. In Desktop, you can execute one program at a time or detach programs so that they run in separate windows. You can also add links that display at the bottom of a program screen that let you start other programs. You should be aware of how these unique features of the Desktop UI interact with using multiple domains.

Because of this ability to detach windows in Desktop, it is possible to run programs in more than one domain at once, as long as you have the appropriate access.

Important While this is possible, it can become confusing. You should limit how and when you do this.

When you log in to QAD Desktop, the current domain is set based on your default domain defined in User Maintenance. The main QAD Desktop page always reflects this current working domain. All new programs that you start also point to this domain. From the Desktop point of view, this is the base domain.

Note Beginning with release 2.7 of QAD Desktop, you can change your domain at any time using the drop-down provided on the QAD Desktop main page.

Figure 2.20 illustrates Sales Order Maintenance running in the base domain of North American Headquarters. The long domain name displays in the Internet Explorer window title and the short domain name displays in the program title bar.

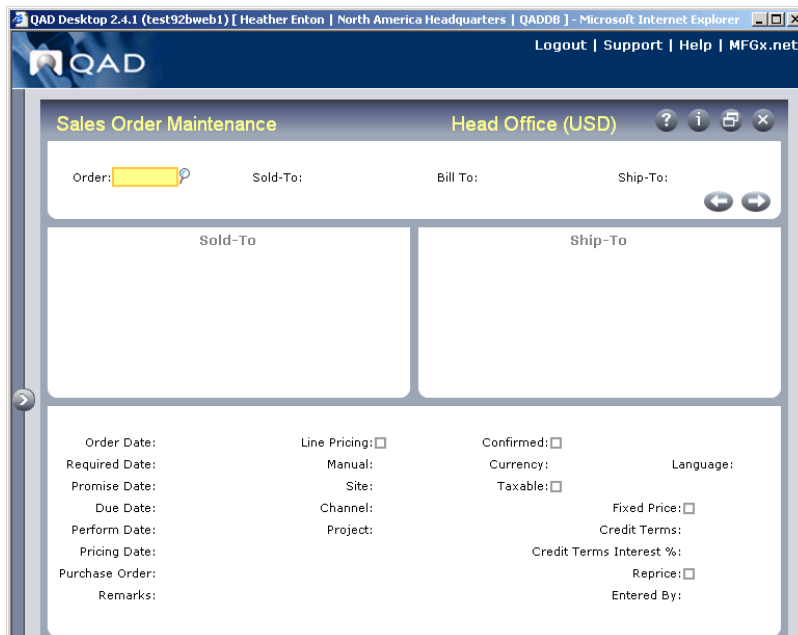


Fig. 2.20
Sales Order
Maintenance in
Head Office
Domain

When you detach a window, the detached window retains the base domain associated with the main Desktop window. Figure 2.21 illustrates Sales Order Maintenance after it has been detached still running in the Head Office Domain.

Fig. 2.21
Sales Order
Maintenance
Detached in Head
Office Domain

The screenshot shows a web browser window titled "Sales Order Maintenance (test92bweb1) [Heather Enton | North America Headquarters | QADDB] - Microsoft Internet ...". The main content area is titled "Sales Order Maintenance" and "Head Office (USD)". It contains several input fields and checkboxes:

- Order: [Yellow box]
- Sold-To: [Empty box]
- Bill To: [Empty box]
- Ship-To: [Empty box]
- Sold-To: [Empty box]
- Ship-To: [Empty box]
- Order Date: [Empty box]
- Required Date: [Empty box]
- Promise Date: [Empty box]
- Due Date: [Empty box]
- Perform Date: [Empty box]
- Pricing Date: [Empty box]
- Purchase Order: [Empty box]
- Remarks: [Empty box]
- Line Pricing: ☐
- Manual: [Empty box]
- Site: [Empty box]
- Channel: [Empty box]
- Project: [Empty box]
- Confirmed: ☐
- Currency: [Empty box]
- Taxable: ☐
- Language: [Empty box]
- Fixed Price: ☐
- Credit Terms: [Empty box]
- Credit Terms Interest %: [Empty box]
- Reprice: ☐
- Entered By: [Empty box]

If you now use Change Current Domain to switch domains, the base domain changes. However, the detached window still references the domain it was started in.

Tip
These domain names are clearly marked on the program title area.

In Figure 2.22, the user has used Change Current Domain to change to domain United Kingdom/Dudley. This is the domain name now displaying in the main Desktop window. A new instance of Sales Order Maintenance started in this window also references the UK / Dudley domain. The original detached window still references the Head Office domain.

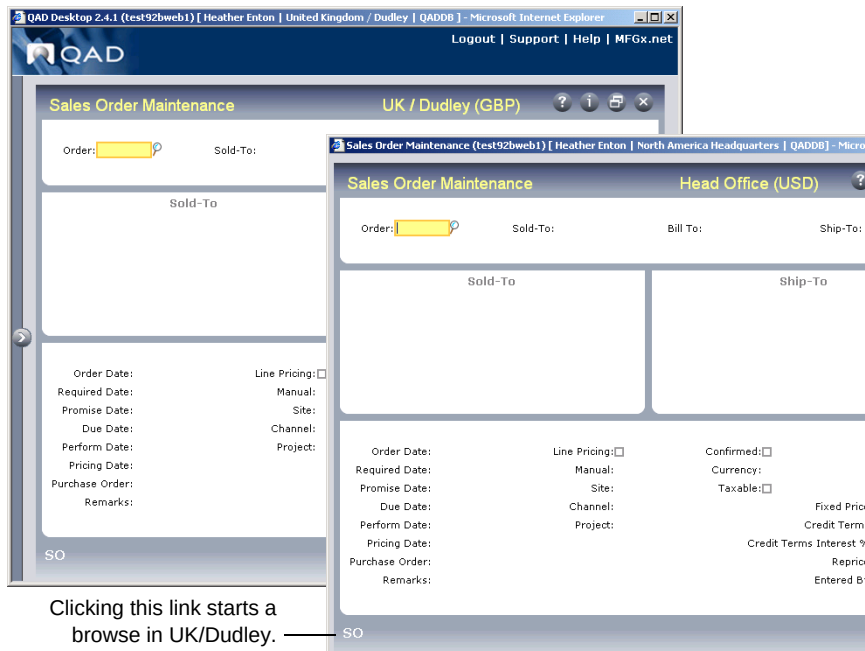
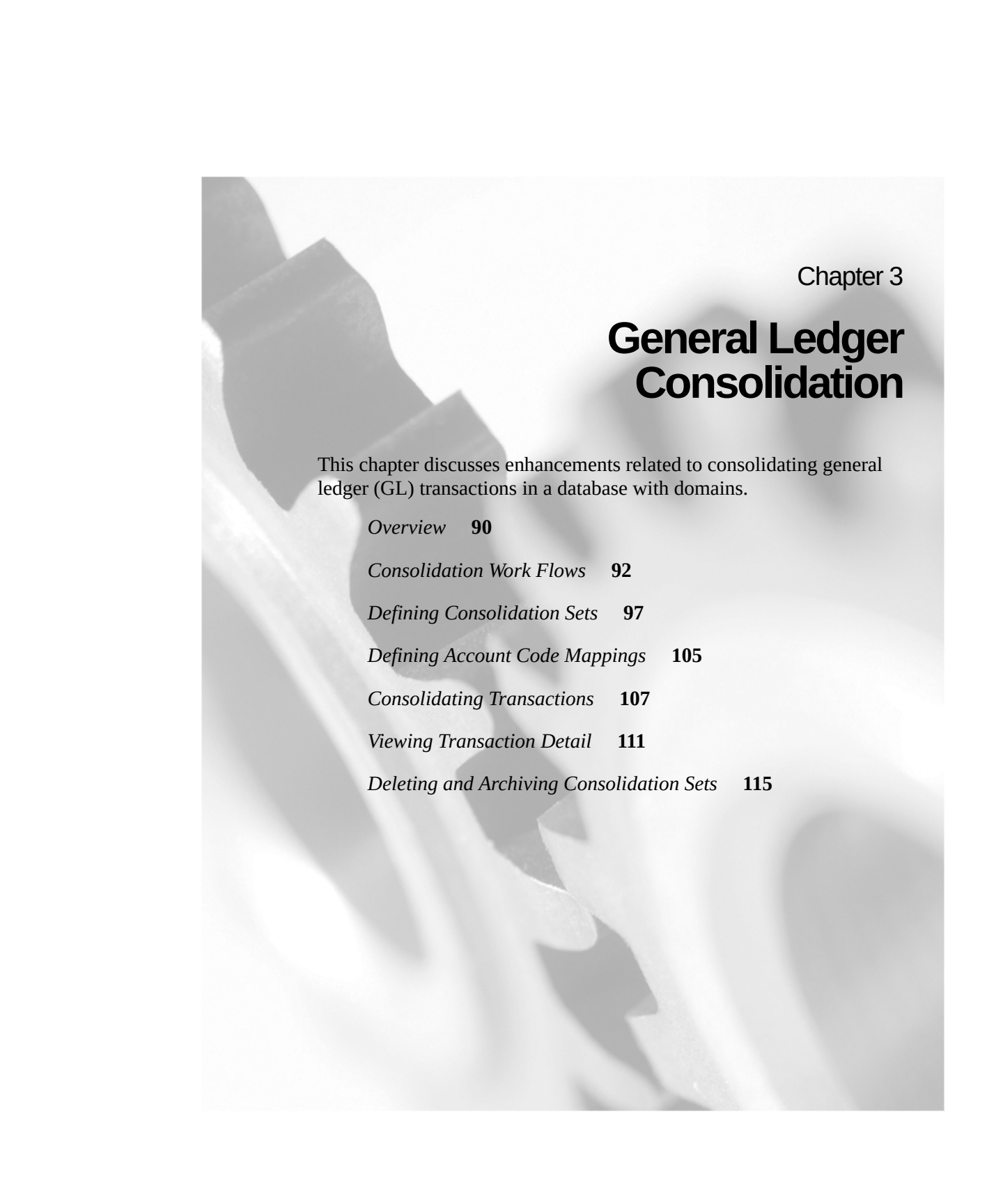


Fig. 2.22
Main Window and
Detached Window
in Two Domains

If you have program links associated with a program that is running in a detached window, programs started using these links follow the standard rule of referencing the base domain, regardless of the domain associated with the program in the detached window.

Example When you click on the link to start Sales Order Browse in the detached window that references the Head Office domain, the new browse window displays sales orders in domain UK / Dudley, since it is now the base domain.

As you can see, this could become confusing. Most users will never encounter this issue because they typically complete activities in one domain only. However, system administrators and other users with access to multiple domains should be aware of how this feature operates.

The background of the page features a grayscale image of several interlocking mechanical gears. The gears are of different sizes and are positioned in a way that creates a sense of depth and motion. The lighting is soft, highlighting the metallic texture and the complex geometry of the teeth.

Chapter 3

General Ledger Consolidation

This chapter discusses enhancements related to consolidating general ledger (GL) transactions in a database with domains.

<i>Overview</i>	90
<i>Consolidation Work Flows</i>	92
<i>Defining Consolidation Sets</i>	97
<i>Defining Account Code Mappings</i>	105
<i>Consolidating Transactions</i>	107
<i>Viewing Transaction Detail</i>	111
<i>Deleting and Archiving Consolidation Sets</i>	115

Overview

Consolidation is typically used when multiple entities must report financial statements in one currency. The introduction of domains and other supporting changes streamlines and enhances the process of GL consolidation among entities in the same domain, in different domains within a single database, and in multiple databases.

The key to this streamlining is the concept of consolidation sets, which define the subsidiary entities that report through a consolidation entity. You can use Entity Code Maintenance (25.3.1.1) to indicate if an entity is a consolidation entity. For consolidation entities, additional frames display that let you specify the subsidiary entities that provide information for consolidated reporting.

All of the entities that belong to a consolidation set must exist in the current database. If you need to consolidate transactions from other databases, you must use Transaction Export (25.19.14) to create an ASCII file of transactions, and then use Transaction Import (25.19.15) to bring the transactions into the corresponding entity in the consolidation database.

Figure 3.1 illustrates the relationships and activities surrounding consolidation. If all of your domains exist in one database, the export/import activities are not needed.

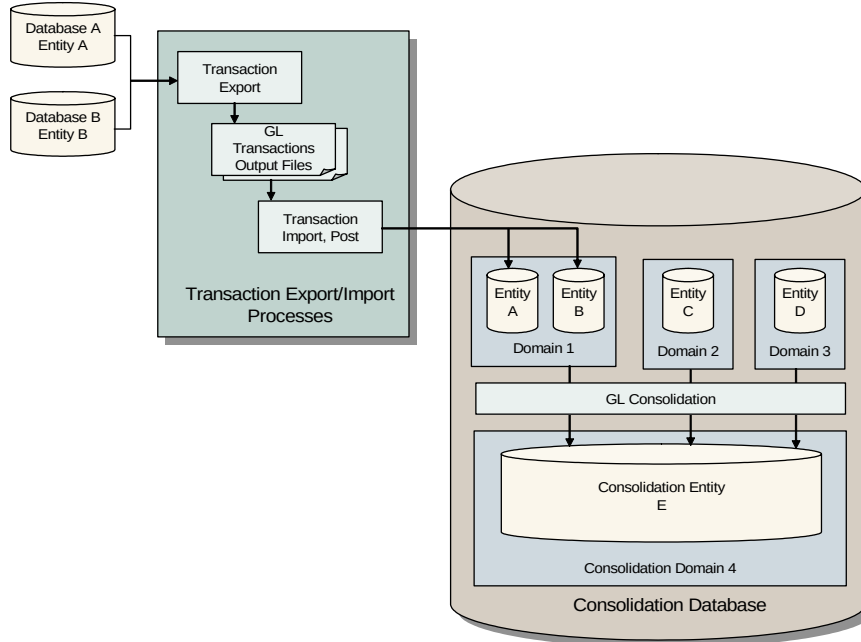


Fig. 3.1
Export/Import and
GL Consolidation

You use GL Consolidation (25.19.20) in the consolidation database to create the transactions for consolidated reporting, based on the relationships set up for a consolidation set in Entity Code Maintenance. This approach minimizes errors, since all of the required information has been set up ahead of time.

Using consolidation sets also has the advantage of letting you model different views of your business. You can create consolidation sets specifically to generate reports and then delete and/or archive the resulting transactions and optionally the consolidation sets using Consolidation Entity Delete/Archive (25.3.1.6) when they are no longer needed.

The GL consolidation process supports consolidation in any of the following conditions:

- Multiple entities within the same domain. Before the introduction of domains, you could generate consolidated reports with selected entities in a database only if the entity codes were in a sequential range. Using consolidation sets, you can select exactly which entities you want to include, regardless of the value of the entity code.

- Multiple entities in more than one domain in a single database. You can combine any number of entities from different domains in a database into a consolidation set. One entity can belong to more than one consolidation set, letting you create multiple views of your business.
- Multiple levels of consolidation. You can add consolidation entities as subsidiaries to a higher-level parent, thereby creating hierarchies with as many levels as you need.
- Multiple entities in more than one database at more than one MFG/PRO release level. Using transaction export and import features, you can import transactions into entities in a target database that are part of a GL consolidation set in preparation for consolidation. The transactions can be imported from databases on the same revision of MFG/PRO or on earlier versions. This facilitates the roll-out and upgrade path, since you do not have to update all remote databases simultaneously.

The following sections discuss:

- Consolidation work flows
- Defining consolidation sets
- Consolidating transactions
- Viewing transaction detail
- Deleting and archiving consolidation sets

Consolidation Work Flows

Before attempting to consolidate transactions, you must complete a number of preparatory steps:

- You must complete all financial activity in the source entities.
- If entities are in different databases, you must follow steps to export transactions from the source database and import them into the consolidation database.
- You must prepare for the consolidation in the consolidation domain.

This section discusses these three sets of activities.

Prepare Source Entities for Financial Reporting

Each subsidiary entity that submits data for consolidation must go through a standard set of preparation steps:

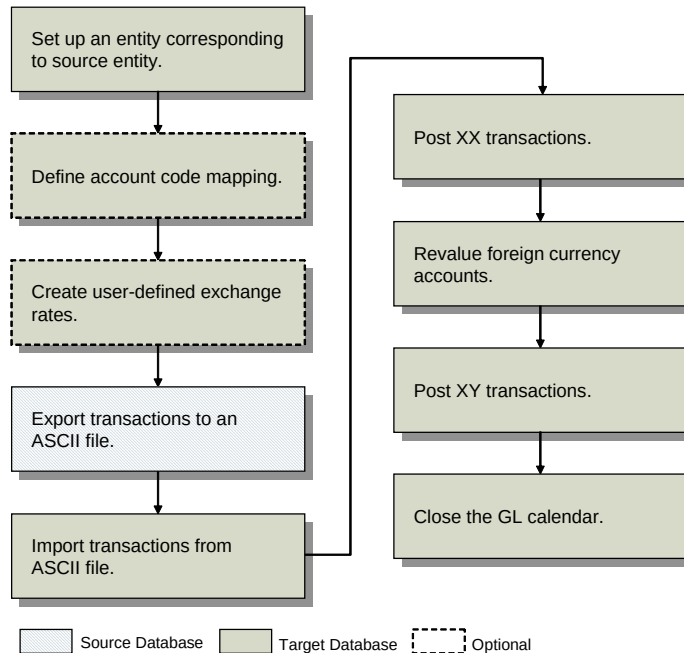
- Post all unposted GL transactions.
- Close the GL calendar period to all modules other than GL using GL Calendar Maintenance (25.3.4).
- Create any corrections or adjustments needed using functions on the GL Transactions menu and post these adjustments.
- If foreign currencies are involved in any GL transactions, revalue these amounts at current exchange rates using Foreign Exchange Revaluation (25.19.13). This creates unrealized gain and loss transactions (FX) that must be posted using Transaction Post (25.13.7).
- Generate and review financial statements using Balance Sheet (25.15.8) and Income Statement (25.15.13).
- After financial reports are reviewed and verified, close the GL period using GL Calendar Maintenance (25.15.8).

Note The system does not require that GL periods are closed in subsidiaries before you can run a GL consolidation. You may need to begin reviewing consolidation reports before you can complete the calendar closure. However, warnings display if the calendar is not closed. Before generating a final consolidation, you should ensure that the calendar is closed.

Export and Import Transactions in Multiple Databases

Figure 3.2 summarizes the steps you must follow to prepare for consolidated reporting when entities exist in different databases. These steps are not required when entities exist within domains in the same database.

Fig. 3.2
Export/Import
Work Flow



To prepare for GL consolidation when entities exist in different databases, follow these steps:

- 1 Set up an entity in the target database with the same name and currency as the entity in the source database. This entity should have Consolidation Entity set to No in Entity Code Maintenance.
- 2 If the source and target entities have different charts of accounts, use From-Account Cross-Reference Maintenance (25.19.4) in the target database and domain to map source accounts to target accounts. Specify a subsidiary entity but leave the consolidation entity blank to define account relationships used by Transaction Import.

Note While the source and target entities may have different charts of accounts, they must have the same GL calendar setup for the import to work correctly.

- 3 If any of your source accounts have a user-defined currency translation index (5 in Account Code Maintenance), use Translation Exchange Rate Maintenance (25.19.1) in the target database and domain to define the appropriate exchange rates for import.
- 4 Use Transaction Export (25.19.14) in the source database to export transaction records for a fiscal period to an ASCII file. Make sure you have completed the steps to prepare an entity for reporting.
- 5 Use Transaction Import (25.19.15) in the target database to import the transactions in the ASCII file into the same subsidiary entity in the current working domain of the consolidation database, creating transactions of type XX. Transaction Import maps accounts and translates currencies as needed.
- 6 Use Transaction Post (25.13.7) to post the imported XX transactions in the target database.
- 7 Use Imported Transaction Revaluation (25.19.17) to revalue any foreign currency accounts.
- 8 Use Transaction Post to post the newly created XY transactions in the target database.
- 9 Close the GL calendar period for the entity holding the imported GL transactions using GL Calendar Maintenance (25.3.4).

◆ See “Prepare Source Entities for Financial Reporting” on page 93.

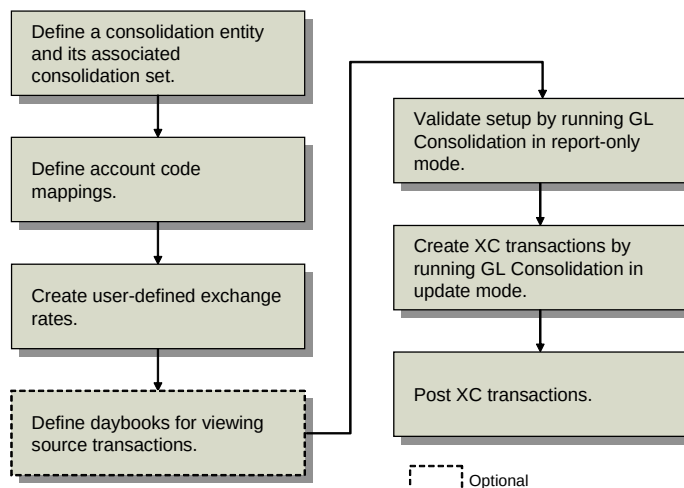
After completing these steps, you are ready to use GL Consolidation (25.19.20) to consolidate the transactions of the subsidiary entity into the consolidation entity or entities defined in Entity Code Maintenance.

Prepare Consolidation Domain

Figure 3.3 summarizes the steps you must follow to prepare for consolidated reporting when entities exist in different domains within the same database. These steps all take place within the consolidation domain.

Note The term *consolidation domain* is used to refer to the domain where consolidation takes place. This can be a domain set up specifically for this purpose only, but this does not have to be the case. You can use a domain that represents an active business operation in the database.

Fig. 3.3
GL Consolidation
Work Flow



See page 97.

- 1 Use Entity Code Maintenance (25.3.1.1) to indicate entities that are used for consolidation, specify the subsidiary entities that are associated with them, and define other settings affecting consolidation such as transaction summarization and consolidation percentage.

See page 105.

- 2 If the subsidiary and consolidation entities are in different domains with different charts of accounts, use From-Account Cross-Reference Maintenance (25.19.4) in the consolidation domain to map subsidiary accounts to consolidation accounts.

Note GL Consolidation does not require that the GL calendar be the same in the source and target domain.

- 3 If any of your subsidiary accounts have a user-defined currency translation index, use Translation Exchange Rate Maintenance (25.19.1) in the consolidation domain to define the appropriate exchange rates to be used during consolidation.
- 4 If you use daybooks, set up daybooks in the consolidation domain for reporting consolidation transactions. Use Default Daybook Maintenance (25.8.4) to set up default daybooks based on the source transaction type and document type. GL Consolidation uses these daybook codes rather than ones associated with transaction type XC. This approach provides support for detailed analysis since consolidation transactions are not all grouped together in one daybook.
- 5 Run GL Consolidation (25.19.20) with Update set to No to generate a list of any setup errors. Correct all these errors before continuing. ▶ See page 107.
- 6 Run GL Consolidation with update set to Yes to consolidate the transactions of the subsidiary entity into the consolidation entity defined in Entity Code Maintenance, creating transactions of type XC. ▶ See page 107.
- 7 Review the results of the consolidation using Unposted Transaction Register (25.13.14). If problems are found, correct them in the subsidiary entity and reexecute GL Consolidation. ▶ See page 108.
- 8 Use Transaction Post (25.13.7) to post the consolidated XC transactions in the consolidation domain.

Defining Consolidation Sets

Use Entity Code Maintenance to set up entities and define consolidation sets. At least one entity code must be defined in each domain.

An entity is an independent financial unit within a domain used for financial reporting. Each entity generates a separate balance sheet and income statement, plans budgets, and is assessed for taxes. All GL transactions are posted by entity. Financial reports for one or multiple entities within a domain are prepared by selecting transactions by entity code.

Note An entity is fully defined by its domain location and entity code. This means that you can have entities with the same name in different domains. This might be required to support some centralized order entry scenarios when the shipping sites are set up in different domains, but actually belong to the same legal entity.

Consolidation Entities

Use the Consolidation Entity field to indicate that an entity is to be used for consolidation activities. When Consolidation Entity is Yes, additional frames display so that you can specify the subsidiary entities that report through the consolidation entity and define a percentage of ownership. The subsidiary entities can belong to any domain in the current database. You cannot reference an entity in another database.

Special restrictions apply to consolidation entities:

- Only transactions created in the GL module can be posted. These include the following types: FX, JL, RA, RV, XC, XX, XY, YR, and YA. You cannot post IC, SO, WO, AP, AR, or CS transactions.
- You cannot associate a consolidation entity with a bank in Bank Maintenance or set the Consolidation Entity field to Yes for an entity associated with a bank.
- You cannot associate a consolidation entity with a site in Site Maintenance or set the Consolidation Entity field to Yes for an entity associated with a site.
- You cannot change the value of Consolidation Entity from Yes to No or No to Yes after GL transactions referencing the entity exist.
- You cannot delete a consolidation entity with this program when GL transactions reference it. Instead, you must use Consolidation Entity Delete/Archive.

Creating Consolidation Sets

You can set up more than one consolidation set to meet your reporting requirements. The same entities can belong to more than one consolidation set if needed. You can also create consolidation hierarchies by referencing a consolidation entity as a subsidiary in a higher level consolidation set.

For example, you have five subsidiary entities: S1 through S5. S1, S2, and S3 are consolidated into consolidation entity C1 and S4 and S5 are consolidated into C2. C1 and C2 are then consolidated into C3, which represents the entire structure.

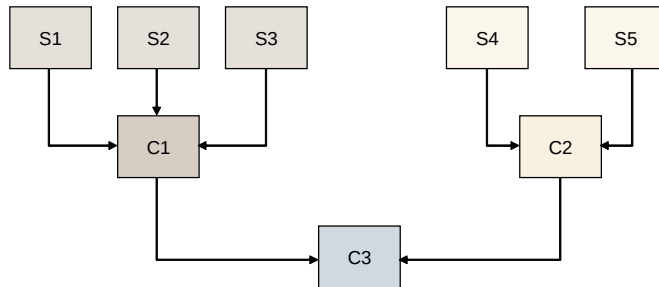


Fig. 3.4
Consolidation
Hierarchy

When you create a structure like this, you cannot reference a subsidiary entity twice, either directly or indirectly. In Figure 3.5, both the shaded relationships cause errors. On the left, S2 cannot be referenced twice for consolidation entity C1 directly. On the right, S1 cannot be referenced twice for consolidation entity C3 indirectly, through C1 and C2.

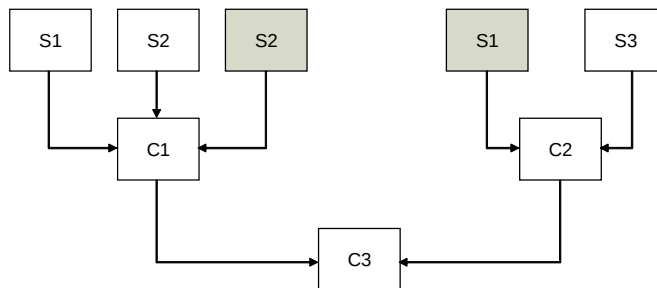


Fig. 3.5
Invalid
Consolidation
Hierarchy

Unlike non-consolidation entities, you can create consolidation sets strictly for reporting different views of a business. Once the reports have been generated and reviewed, the transactions and even the model on which they were based may no longer be needed. In this case you can use Consolidation Entity Delete/Archive (25.3.1.6) to delete and optionally archive the transactions and the data associated with the consolidation entity.

► See “Deleting and Archiving Consolidation Sets” on page 115.

Entity Code Maintenance

Figure 3.6 illustrates fields related to consolidation in Entity Code Maintenance (25.3.1.1).

Fig. 3.6
Entity Code
Maintenance
(25.3.1.1)

The screenshot shows the 'Entity Code Maintenance' window for 'Head Office (USD)'. The fields displayed are:

- Entity: 2020
- Description: [Yellow input field]
- Primary Entity: [Yellow input field]
- Currency: USD
- Post Translation Adj to (B/I): Bal Sheet
- Posting Audit Trail Page Nbr: 0
- Company Address: 10000
- Consolidation Entity: ☒ (This field is highlighted with a black box and a line pointing to the label 'Consolidation fields' below the window)
- Type: Consol

At the bottom right of the window are three buttons: a red 'X' (close), a left arrow (previous), and a right arrow (next).

Consolidation Entity. Indicate if this entity is used for GL consolidation.

No: This is a standard entity that is not used for creating consolidated financial reports.

Yes: This is a consolidation entity. Additional frames display in which you can specify the subsidiary entities that are part of the GL consolidation and assign each a consolidation percentage. When you specify Yes, the system verifies that the entity is not currently associated with a bank or a site.

Entity Type. Enter a code identifying the entity type. The system validates this field against values defined in Generalized Codes Maintenance for field en_type.

Use type codes to group related entities for consolidation. You can select subsidiary entities to be part of a consolidation entity by type code.

Examples of entity types could include:

- Fully owned subsidiary
- Associated company
- Local GAAP entity
- US GAAP entity
- Common GAAP entity

When you indicate that an entity is a consolidation entity, additional screens display. You can add subsidiary entities one at a time or select multiple entities based on various criteria. The screen navigation varies depending on your choice.

The screenshot shows the 'Entity Code Maintenance' window for 'Head Office (USD)'. At the top, it displays 'Consolidation Entity: 2020', 'Curr: USD', and 'Type: Consol'. Below this is a table with columns: Sub Ent, Sub Domain, CE, Entity T, Base, Sum, Cons%, and Description. A 'Select Option' dialog box is open, asking 'Enter selection' with two buttons: '1' and '2'.

Fig. 3.7
Entity Code
Maintenance,
Assigned
Subsidiaries

Option. Enter 1 if you want to specify subsidiary entities one at a time.

Enter 2 if you want to choose from a group of entities based on selection criteria that you specify, such as range of domains, entity codes, entity types, or currencies.

If you choose 1 (Single), the Assigned Subsidiaries frame displays (see Figure 3.11). Use the Add key or command to display the Add Subsidiary frame as in Figure 3.8.

The screenshot shows the 'Entity Code Maintenance' window for 'Head Office (USD)'. It displays the same top information as Figure 3.7. Below the table header, there is one row of data:

Sub Ent	Sub Domain	CE	Type	Curr	Sum	Cons%	Description
2000	demo1				✓	100.00%	

At the bottom right of the table, there are three buttons: a red 'X', a left arrow, and a right arrow.

Fig. 3.8
Entity Code
Maintenance, Add
Subsidiary

Specify values in the following fields:

Subsidiary Entity. Enter a code identifying an entity that forms part of this GL consolidation set. The entity must belong to the specified subsidiary domain.

You can include the same source entity in more than one consolidation set, to support multiple reporting views of your business. However, you cannot reference the same entity more than once in this consolidation set, either directly or indirectly.

Note The same entity code can be referenced twice only if it is associated with different domains.

Subsidiary Domain. Enter the domain code of the subsidiary entity in a GL consolidation set. This code must be a valid, active domain associated with the current database and assigned to your ID in User Maintenance.

Note You cannot reference a domain associated with a connected database.

Summarize. Indicate whether posted GL transactions in the subsidiary entity are consolidated as detailed or summarized unposted transactions in the consolidation entity.

No: Each GL transaction is consolidated in detail.

Yes: The system summarizes all positive GL transactions for the same daybook code or project code (and matching account, sub-account, and cost center) into a single unposted debit GL transaction. All negative GL transactions are summarized into one credit transaction.

Consolidation Percentage. Specify the percentage of the subsidiary entity transactions that will be consolidated into the general ledger of the consolidation entity. The default is 100%. This value cannot be over 100%.

Typically, when a subsidiary entity is more than 51% owned by the parent company, 100% of the subsidiary transactions are shown in the books of the consolidation entity. However, when ownership is less than 51% and the national accounting rules permit it, proportional consolidation can be used.

In this case, enter the actual ownership percentage in this field. GL Consolidation then multiplies the amounts of the subsidiary entity GL transactions by this percentage.

Even when you set Summarize to Yes, detail about individual transactions is retained for historical reporting. Use Inquiry by Account with Drill Down (25.13.20) to view these details as needed.

Note This setting has no effect on accounts defined with a currency translation index of 4 (historical). Transactions for these accounts are never summarized.

Press Go to add the entity. It displays in the frame above. You can add as many entities as you want to this consolidation set.

If you choose 2 (Multi), the frame in Figure 3.9 displays.

▶ See “Viewing Transaction Detail” on page 111.

The screenshot shows the 'Entity Code Maintenance' window for 'Head Office (USD)'. The top section displays 'Source Domain: demo1', 'North America Headquarters', 'Curr: USD', 'Consolidation Entity: 2020', and 'Type: Consol'. The bottom section, titled 'Subsidiary Multi Selection', contains several input fields: 'Subsidiary Domain:', 'Subsidiary Entity:', 'Entity Type:', and 'Currency:', each followed by a yellow input box and a magnifying glass icon. To the right, there are four 'To:' labels, each followed by a yellow input box and a magnifying glass icon. Below these fields are two checkboxes: 'Include Consolidation Entities:' and 'Select All:'. At the bottom right, there are three buttons: a red 'X' button, a left arrow button, and a right arrow button.

Fig. 3.9
Entity Code
Maintenance,
Subsidiary Multi
Selection

When you add multiple entities, you enter selection criteria for a range of domains, entities, entity types, and currencies. You can choose to include or exclude consolidation entities in the selection. You can also specify whether the matching entities should be selected by default for inclusion in the set.

Note Only entities that belong to the current database display for selection, regardless of the range you enter.

Include Consolidation Entities. Enter No if you want to exclude entities with Consolidation Entity set to Yes; otherwise, enter Yes.

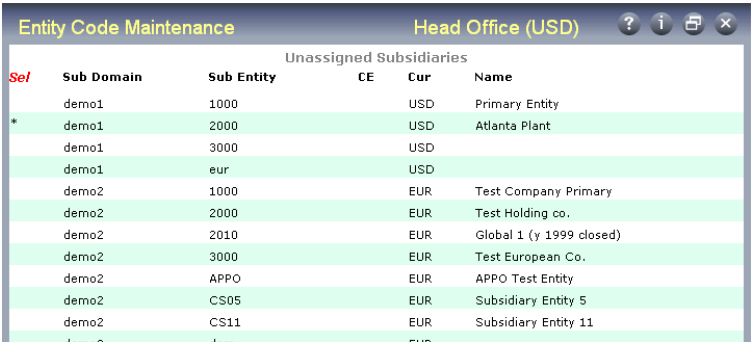
Select All. Indicate whether you want entities that match the selection criteria to be selected by default.

No: Matching entities display unselected in the next frame. You must select the ones you want.

Yes: Matching entities display already selected in the next frame. You can simply press Go to continue.

When you press Go, the search results display in a screen like the one in Figure 3.10. You can then select or deselect individual entities as needed.

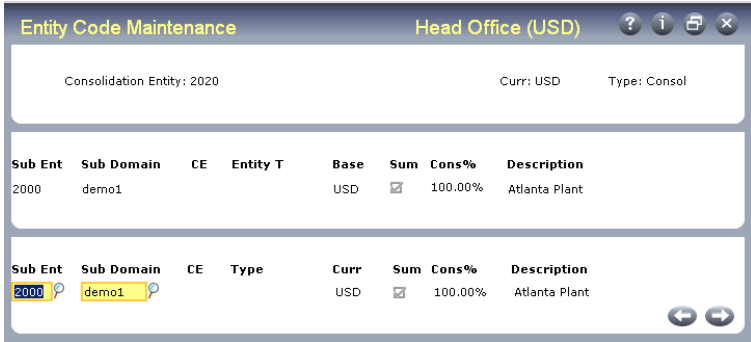
Fig. 3.10
Entity Code
Maintenance,
Unassigned
Subsidiaries



Sel	Sub Domain	Sub Entity	CE	Cur	Name
	demo1	1000		USD	Primary Entity
*	demo1	2000		USD	Atlanta Plant
	demo1	3000		USD	
	demo1	eur		USD	
	demo2	1000		EUR	Test Company Primary
	demo2	2000		EUR	Test Holding co.
	demo2	2010		EUR	Global 1 (y 1999 closed)
	demo2	3000		EUR	Test European Co.
	demo2	APPO		EUR	APPO Test Entity
	demo2	CS05		EUR	Subsidiary Entity 5
	demo2	CS11		EUR	Subsidiary Entity 11

When you press Go again, all selected entities are added to the consolidation set and display in the Assigned Subsidiaries frame.

Fig. 3.11
Entity Code
Maintenance,
Assigned
Subsidiaries



Sub Ent	Sub Domain	CE	Entity T	Base	Sum	Cons%	Description
2000	demo1			USD	☒	100.00%	Atlanta Plant

You can modify the summarization value and consolidation percentage in this frame as needed.

Note If the subsidiary entity is also a consolidation entity in another consolidation set, an asterisk (*) displays in the CE (Consolidation Entity) column.

Viewing Consolidation Information

You can use either of the following programs to view information about consolidation sets:

- Use Entity Consolidation Detail Inquiry (25.19.10) to view a list of subsidiary entities related to a consolidation entity and associated information.
- Use Entity Consolidation Detail Report (25.19.11) to view a similar list in report format. This report lets you optionally explode subsidiary entities that are themselves consolidation entities, producing an indented listing of the consolidation hierarchy.

Defining Account Code Mappings

Use From-Account Cross-Reference Maintenance (25.19.4) to create relationships between accounts in different entities to be used during transaction import and GL consolidation:

- Transaction Import uses this data to map accounts associated with GL transactions created for an entity in a source database to accounts for the same entity in the target database.
- GL Consolidation uses this data to post transactions from a subsidiary entity and domain within the current database into the correct corporate accounts in the consolidation entity.

Note If you do not perform GL consolidation, cross-reference information is not used.

Figure 3.12 illustrates From-Account Cross-Reference Maintenance.

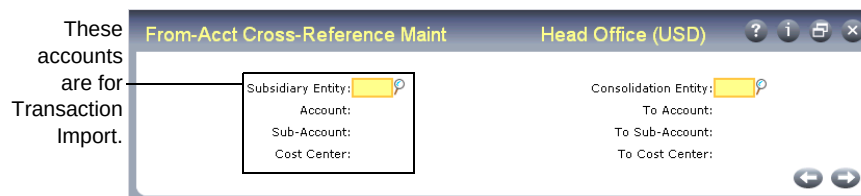


Fig. 3.12
From-Account
Cross-Reference
Maintenance
(25.19.4)

You fill in different fields depending on whether you are setting up mappings to be used during import or consolidation.

- When you set up cross-references to be used by Transaction Import, specify a subsidiary entity but leave the consolidation entity blank. The source and target entity during import is always the same.
- When you set up cross-references to be used by GL Consolidation, you must specify both a consolidation entity and a subsidiary entity. GL Consolidation always takes place between two different entities in the same database.

The validations for the entity and account fields vary depending on the type of cross-references you are setting up:

- For Transaction Import, the subsidiary entity and To accounts must exist in the current domain. From accounts are not validated since they are in a different database.
- For GL Consolidation, the subsidiary entity must exist in the subsidiary domain as defined for the consolidation set defined in Entity Code Maintenance. From accounts are validated in that domain and To accounts are validated in the current working domain.

During import or consolidation, the system reads the account, sub-account, and cost center from the source transaction and looks for a match in the cross-reference table of the consolidation entity's domain. It searches for a match in the following order:

- 1 Matching account, sub-account, and cost center
- 2 Matching account, sub-account, and blank cost center
- 3 Matching account, blank sub-account, and blank cost center

If no matches are found, the transaction is posted to the same account specified on the originating transaction. If this account does not exist, errors are generated.

Consolidating Transactions

Use GL Consolidation (25.19.20) to load transactions with a range of effective dates from subsidiary entities as unposted XC transactions in a consolidation entity. You can post these transactions in the consolidation domain in preparation for creating consolidated financial reports.

Note Consolidation is single level; it is not recursive. If a consolidation set includes subsidiary entities that are also consolidation entities, you must execute the lower-level consolidations first.

Validating GL Consolidation Setup

Executing GL Consolidation with Update set to No generates a report listing any setup errors or warnings. Warnings are generated when the following conditions exist in one of the subsidiary entities for the consolidation period:

- The calendar is not closed.
- Unposted GL transactions exist.

These conditions produce warnings rather than errors since you may need to begin reviewing consolidation reports before you complete posting and close the calendar. Before generating a final consolidation, you should ensure that transactions are posted and the calendar closed in each subsidiary.

An error is generated when account/sub-account/cost center combinations are defined in the subsidiary entity that do not exist in the consolidation entity and no mappings are defined in From-Account Cross-Reference Maintenance. Correct this error before continuing.

Consolidation Processing

During consolidation, the following updates are made:

Summarization. Consolidated transactions are created as summarized or in detail based on the setting of Summarize for each subsidiary entity in the consolidation set defined in Entity Code Maintenance.

Even when summarized GL transactions are created, details are retained for reporting in Inquiry by Account with Drill Down (25.13.20).

◆ See “Defining Account Code Mappings” on page 105.

Account Cross-Referencing. If an account referenced in the subsidiary transaction does not exist in the consolidation domain, the system searches for alternate accounts defined in From-Account Cross-Reference Maintenance and changes the numbers to the consolidation entity numbering scheme. If a cross-reference does not exist, an error is generated.

Currency Translation. Subsidiary accounts with amounts expressed in a non-base currency are translated to the currency of the entity in the consolidation database. If the currency translation index for an account is 5, the system looks for a valid exchange rate specified in Translation Exchange Rate Maintenance (25.19.1). The exchange rate relationship is used to convert the amount from the account currency to the base currency.

Unposted Consolidation Transactions. During consolidation, the system changes the domain and entity of the transactions to the consolidation domain and entity specified. It multiplies the amount of the transaction by the consolidation percent specified for the subsidiary entity in Entity Code Maintenance before creating the XC transactions.

Rounding Differences. To prevent the creation of unbalanced transactions, any rounding differences in the consolidation process update the Translation Adjustment Account (BS) or the Translation Adjustment Account (IS) from General Ledger Control, depending on the setting of Post Translation Adjustment to (B/I) in Entity Code Maintenance. Multiple transactions can be created, one for each daybook affected.

Correcting Consolidation Transactions

When you run GL Consolidation in update mode and errors prevent an XC transaction from being created, you can correct the error and rerun the function with Reprocess set to Yes. In this case, the system creates XC transactions only for transactions that previously failed to be consolidated.

After XC transactions are created, you cannot use Standard Transaction Maintenance (25.13.1) to correct them. If errors are found after consolidation, correct the transaction in the subsidiary and rerun the consolidation.

Completing Steps after a Consolidation

After completing a consolidation, you should continue with these steps:

- 1 Use Transaction Post to post the consolidation (XC) transactions for the consolidation entity.
- 2 Use Foreign Exchange Revaluation (25.19.13) to revalue amounts for GL accounts defined in currencies other than the base currency of the consolidation entity. Post any resulting FX transactions.
- 3 Use Imported Transaction Revaluation (25.19.17) to revalue any consolidated transactions for accounts in the consolidation entity that have a Currency Translation Index of 1 (current). Post any resulting XY transactions.
- 4 Close the GL calendar period to additional transactions using GL Calendar Maintenance (25.3.4).

Executing GL Consolidation

Figure 3.13 illustrates GL Consolidation (25.19.20).

The screenshot shows a software window titled "GL Consolidation" with a subtitle "Head Office (USD)". The window contains several input fields and buttons:

- Consolidation Entity:** A text field with a search icon.
- Transaction Date:** A date field set to 08/01/2003.
- To:** A date field set to 08/30/2003.
- Consolidation Effective Date:** A date field set to 09/30/2003.
- Update:** A checkbox.
- Reprocess:** A checkbox.
- Output:** A text field.
- Batch ID:** A text field.

At the bottom right, there are two circular buttons with arrows pointing left and right.

Fig. 3.13
GL Consolidation
(25.19.20)

Consolidation Entity. Enter the code identifying the entity that will hold the results of the GL consolidation.

The system validates that:

- This is a valid entity in the current working domain.
- It is defined with Consolidation Entity set to Yes in Entity Code Maintenance.
- At least one subsidiary domain has been specified for it in Entity Code Maintenance.

Transaction Date/To. Specify the beginning and ending dates the system should use for selecting posted transactions in the subsidiary entities of the consolidation set.

The system checks the following conditions for the range of effective dates specified:

- The GL calendar is closed in all subsidiary entities.
- No unposted GL transactions exist in any subsidiary entity.

Consolidation Effective Date. Specify the effective date the system should use for the unposted GL consolidation transactions.

This field defaults to the end date of the current working domain's calendar. You can modify it to another date, but the effective date must be within an open calendar period for the consolidation entity.

Update. Enter Yes to run this program in update mode and change records in the database.

Enter No to run this program in report-only mode without updating the database. A report prints for review with SIMULATION displayed at the top of each page.

When you set update to No, the report includes information about all of the validations that occur. You can correct potential errors and rerun the program with Update set to No until no more errors are generated. Then set Update to Yes to create the GL transactions.

Reprocess. Enter Yes if you want to consolidate only transactions that previously failed because of an error condition; otherwise, enter No.

When you run GL Consolidation in update mode and errors prevent an XC transaction from being created, you can correct the error and rerun the function with Reprocess set to Yes. In this case, the system creates XC transactions only for transactions that previously failed to be consolidated.

Viewing Transaction Detail

Use Inquiry by Account with Drill-Down (25.13.20) to review summarized and detailed transaction information regarding consolidated transactions.

This section illustrates consolidation transactions created based on the business scenario summarized in Table 3.1. Three subsidiary domains create transactions that are consolidated into the Q-CO entity in the consolidation domain QCorp.

Domain	Entity	Currency	Transaction Detail	Consolidating Entity?
QCorp	Q-CO	USD	Summarized	Yes
QFrance	Q-FR	EUR	Summarized	No
QJapan	Q-JP	JPY	Summarized	No
QUK	Q-UK	GBP	Detailed	No

Table 3.1
Consolidation
Scenario

Summarized Transactions

The following sequence of screens illustrates drilling down on summarized transactions created by entity Q-JP. The inquiry is directed against account 5050.

The screenshot shows a software interface titled "Inquiry by Acct with Drill-Down" for "Corp Consolid (USD)". It features several input fields: "Enty" with the value "Q-CR", "Account" with "5050", "Sub-Acct", "CC", "Project", "Daybook" with "Stock", "TT", and "Eff Date" with "01/01/2003". Above the "CC" and "Project" fields is a section labeled "Corporate Corrections". There are also icons for help, information, and a search function, along with navigation arrows at the bottom right.

Fig. 3.14
Inquiry by Account
with Drill Down
(25.13.20)

Figure 3.15 illustrates GL transactions created in the consolidating entity. The column labeled Enty indicates the subsidiary entity associated with the transaction.

Fig. 3.15
Transactions in
Consolidating
Entity

Inquiry by Acct with Drill-Down						
Corp Consolid (USD)						
Corporate Corrections						
Enty	Account	Sub-Acct	CC	Project	Daybook	TT
Q-CO	5050				stock	
Domain : QCorp						
GL Reference	Eff Date	Batch	Enty	Document	Do	Amount
XC030916000003	01/31/2003		Q-FR		XS	1,428.97
XC030916000006	01/31/2003		Q-JP		XS	33,028.20
XC030916000014	01/31/2003		Q-UK		XD	1,065.69
XC030916000015	01/31/2003		Q-UK		XD	1,065.69
XC030916000016	01/31/2003		Q-UK		XD	1,065.69

The column labeled DO (document type) displays XS or XD, depending on the setting of Summarize in Entity Code Maintenance for the subsidiary entity in the consolidation set.

- The document type for summarized transactions created by Q-FR and Q-JP is XS.
- The type for the detailed documents for Q-UK is XD.

Selecting the second summarized reference created by entity Q-JP displays the screen in Figure 3.16.

Fig. 3.16
Details of a
Summarized XC
Transaction

Inquiry by Acct with Drill-Down						
Corp Consolid (USD)						
G/L Transaction List						
GL Reference	Eff Date	Entered	User ID	Description		
XC03091600000	01/31/2003	09/16/2003	imh	CR Q-JP 30/01/03		
Line	Domain	Enty	Account	Amount	Currency Amount	Cur
1	QJapan	Q-JP	1500	-33,028.20	-3540,000.00	JPY
2	QJapan	Q-JP	2250	-33,028.20	-3540,000.00	JPY
3	QJapan	Q-JP	5050	33,028.20	3540,000.00	JPY
4	QJapan	Q-JP	5100	33,028.20	3540,000.00	JPY

This screen shows all of the lines of the XC transaction. The source domain and entity (QJapan and Q-JP) display. Selecting line 3 displays the screen shown in Figure 3.17.

GL Reference	Eff Date	Batch	Enty	Document	Do	Amount
IC030130000002	01/30/2003		Q-JP	3437	IC	1,180,000.00
IC030130000003	01/30/2003		Q-JP	3438	IC	1,180,000.00
IC030130000004	01/30/2003		Q-JP	3439	IC	1,180,000.00

Fig. 3.17
Detailed IC
Transactions in
Domain QJapan

This screen shows the three IC transactions in entity Q-JP in domain QJapan that were combined into a single XS consolidation transaction. The system has switched domains, as indicated in the frame title. If you use the Pivot command to activate the Document column, you can select document 3437 to view its detail, as shown in Figure 3.18.

Tip
You must have access to the source domain to see this detail.

Inquiry by Acct with Drill-Down		Corp Consolid (USD)
Tran Nbr: 3437	Order: 20009	402588
Trans Type: ISS-SO	Revision: 0	
Date: 09/16/2003	Item Number: 10-15000	
Time: 03:55	Description: NOMAD(TM) COOLING SYS	
Effective Date: 01/30/2003	Unit of Measure: EA	
Remarks: 20005	Address: 293029	
User ID: imh	Name: Recourt S.A.	
Program: sosois.p	Sales/Job: 20009	
Currency: JPY	Ship Type:	
Qty Change: -10.0	Price: 59,000.00	
Shipper Number:	Inv Mov:	
Ship Date:		

Fig. 3.18
Document Detail

Detailed Transactions

The following sequence of screens illustrates drilling down on detailed transactions created by entity Q-UK. The inquiry is directed against account 2100.

Figure 3.19 shows all transactions for this account.

Fig. 3.19
Transactions in
Consolidating
Entity for Account
2100

Inquiry by Acct with Drill-Down						
Corp Consolid (USD)						
Corporate Corrections						
Enty	Account	Sub-Acct	CC	Project	Daybook	TT
Q-CO	2100					01/01/2003
Domain : QCorp						
GL Reference	Eff Date	Batch	Enty	Document	Do	Amount
XC030916000001	01/31/2003		Q-CR		XS	2,000.00cr
XC030916000002	01/31/2003		Q-FR		XS	1,428.97cr
XC030916000005	01/31/2003		Q-JP		XS	33,028.20cr
XC030916000008	01/31/2003		Q-UK		XD	1,065.69cr
XC030916000009	01/31/2003		Q-UK		XD	1,065.69cr
XC030916000010	01/31/2003		Q-UK		XD	1,065.69cr

Selecting the fifth reference created by entity Q-UK displays the screen in Figure 3.20.

Fig. 3.20
Consolidation
Transaction from
Entity Q-UK

Inquiry by Acct with Drill-Down						
Corp Consolid (USD)						
G/L Transaction List						
GL Reference	Eff Date	Entered	User ID	Description		
XC030916000000	01/31/2003	01/17/2003	imh	Q-UK 17/01/03		
Line	Domain	Enty	Account	Amount	Currency Amount	Cur
1	QUK	Q-UK	2100	-1,065.69	-670.00	GBP
2	QUK	Q-UK	2250	1,065.69	670.00	GBP

This screen shows both lines of the consolidation transaction. Selecting the line for account 2100 displays the screen shown in Figure 3.21.

Fig. 3.21
Original Subsidiary
Transaction in
QUK

Inquiry by Acct with Drill-Down						
Corp Consolid (USD)						
Domain : QUK						
GL Reference	Eff Date	Batch	Enty	Document	Do	Amount
AP030117000004	01/17/2003	3002	Q-UK	3003	VO	670.00cr

The system switches to the QUK domain. In this case, since the transaction is detailed, a one-to-one relationship exists between the consolidation transaction and the original subsidiary transaction. If you Pivot to the Document column and select the transaction, the screen in Figure 3.22 displays the document detail.

Tip
You must have access to the source domain to see this detail.

The screenshot shows a software window titled "Inquiry by Acct with Drill-Down" with a subtitle "Corp Consolid (USD)". The window displays details for an "Accounts Payable" transaction. The top section contains fields for Reference (3003), Invoice (H3001), Transaction Type (Voucher), Date (01/17/2003), Amount (1,118.67), Effective (01/17/2003), Account (2100), Entity (Q-UK), and Supplier (512023). Below this, a "Distribution" table is shown with columns: Ln, Account, Sub-Acct, CC, Project, Entity, Description, and Amount. The table contains one row with Ln 1, Account 2250, Sub-Acct blank, CC blank, Project blank, Entity Q-UK, Description EXPENSED ITEM RE, and Amount 670.00. The window has standard OS controls (help, info, print, close) in the top right corner.

Ln	Account	Sub-Acct	CC	Project	Entity	Description	Amount
1	2250				Q-UK	EXPENSED ITEM RE	670.00

Fig. 3.22
Document Detail

Deleting and Archiving Consolidation Sets

Use Consolidation Entity Delete/Archive (25.3.1.6) to:

- Delete and optionally archive posted and unposted consolidation GL transactions and supporting detail maintained in the following tables: GL Unposted Detail (glt_det), GL Currency Total Detail (glct_det), GL Transaction History (gltr_hist), and GL Entity Consolidation Detail (glec_det).
- Delete and optionally archive static data associated with a consolidation entity maintained in Entity Master (en_mstr) and Entity Consolidation Detail (encl_det).

Figure 3.23 illustrates Consolidation Entity Delete/Archive.

Fig. 3.23
Consolidation
Entity Delete/
Archive (25.3.1.6)

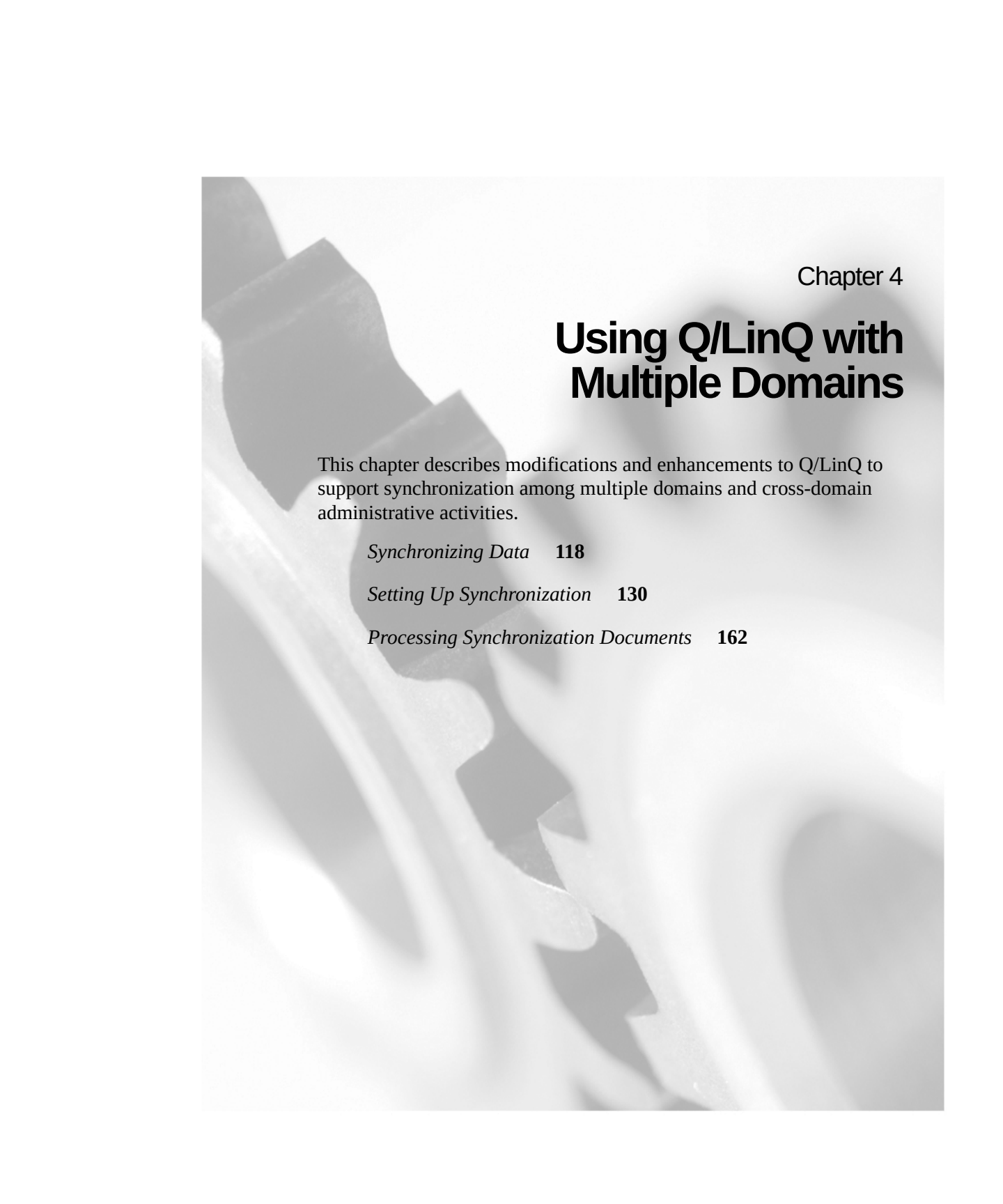


You must delete transactions before you can delete static data.

This function applies only to transactions associated with entities that have Consolidation Entity set to Yes in Entity Code Maintenance. For a non-consolidation entity, transactions are typically retained a number of years; six or seven is a typical legal requirement. In this case, you can use Transaction Summarization (25.13.11) to reduce the number of transactions in the system, rather than delete/archive.

Consolidation entities have a different purpose, since you can create consolidation sets strictly for reporting different views of a business. Once the reports have been generated and reviewed, the transactions and even the model on which they were based may not be needed. In this case you can archive and delete the transactions. If you think you might need to regenerate the report at a future time, you can leave the static data and just delete the transactions.

You should run this function twice. First, run it with Delete set to No and review the report. Then, run it with Delete set to Yes.



Chapter 4

Using Q/LinQ with Multiple Domains

This chapter describes modifications and enhancements to Q/LinQ to support synchronization among multiple domains and cross-domain administrative activities.

Synchronizing Data **118**

Setting Up Synchronization **130**

Processing Synchronization Documents **162**

Synchronizing Data

You can use features of Q/LinQ to synchronize static data such as item master data among multiple domains, both within a single database and between multiple, distributed MFG/PRO databases. The data fields—called the *payload*—and the specific records to be updated—the *filter* or selection criteria—are specified in a *synchronization profile*.

When data included in a synchronization profile changes—either through addition, deletion, or modification—the event is captured using database *schema triggers*, which publish the captured and filtered data to Q/LinQ as export synchronization documents.

► See *External Interface Guide: Q/LinQ* for details on how Q/LinQ works.

Each document represents a single add, change, or delete action for a specific master table record. These documents can be viewed and reported on in the same way as other Q/LinQ documents.

Data Flow

The flow of data during synchronization varies depending on the method used.

- Using one of the Q/LinQ data communications APIs is required when domains are distributed across multiple databases. An API can also be used when a single database has many domains.
- A streamlined forwarding method can be used for synchronizing data among domains in a single database. This is known as *intra-database forwarding*.

Data flow is simpler using intra-database forwarding.

Synchronization Through Q/LinQ Stream or Messaging API

Figure 4.1 illustrates the flow of data during synchronization between domains that communicate with each other through one of the Q/LinQ APIs.

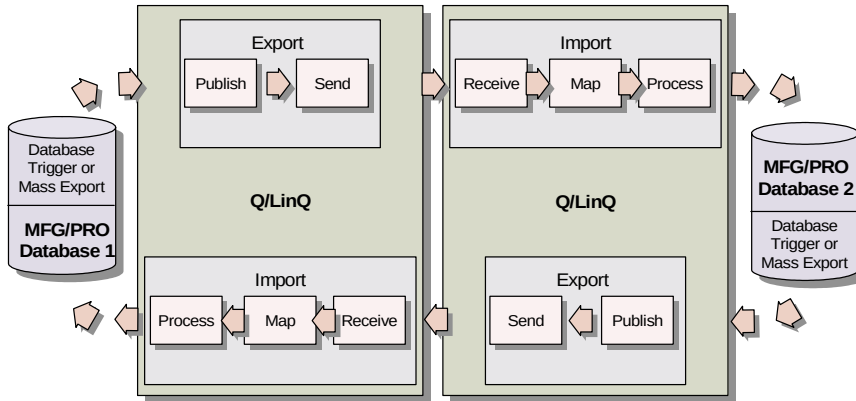


Fig. 4.1
Data Flow Between
Databases Using
APIs

When a table included in a synchronization profile is updated in a source MFG/PRO domain, Q/LinQ publishes the data to an export document and exports that document to Q/LinQ in a destination MFG/PRO database. The destination Q/LinQ receives the document, maps the data, and processes the data in the destination domain.

Figure 4.2 illustrates synchronization relationships among the domains.

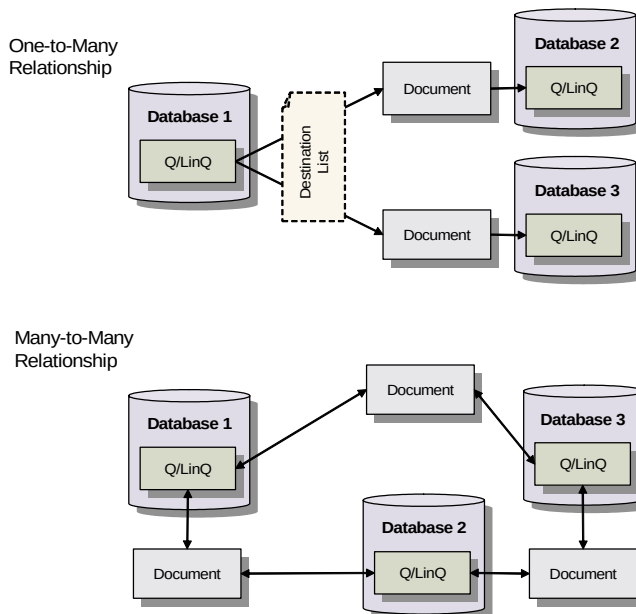


Fig. 4.2
Relationships
Among Domains in
Different Databases

Source and destination domains can be in one-to-one, one-to-many, and many-to-many relationships. A source domain can synchronize different tables with different destination domains or different fields from the same table with different destination domains. In a one-to-many relationship, a destination list can manage the multiple export destinations.

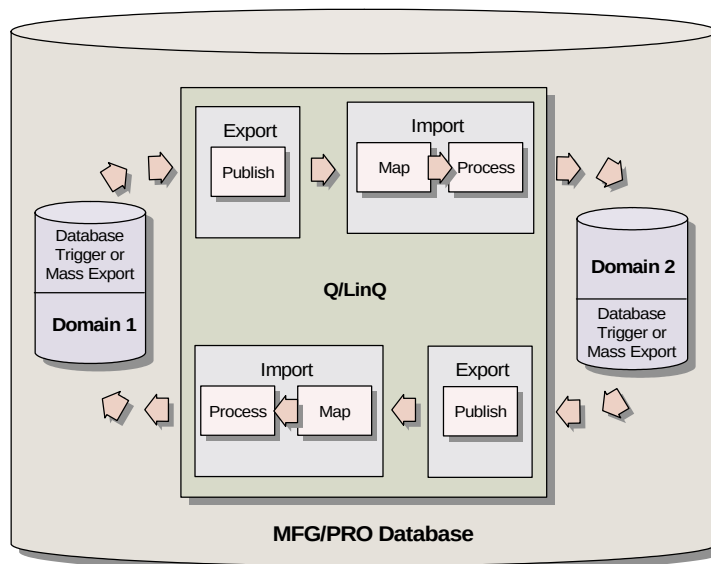
Note Although the figures illustrate domains in different databases, this method can also be used for domains within a single database.

Synchronization Through Q/LinQ Forwarding

Figure 4.3 illustrates the flow of data during synchronization between domains in a single database using Q/LinQ intra-database forwarding.

Note This method of synchronization can be used with domains in a single database only.

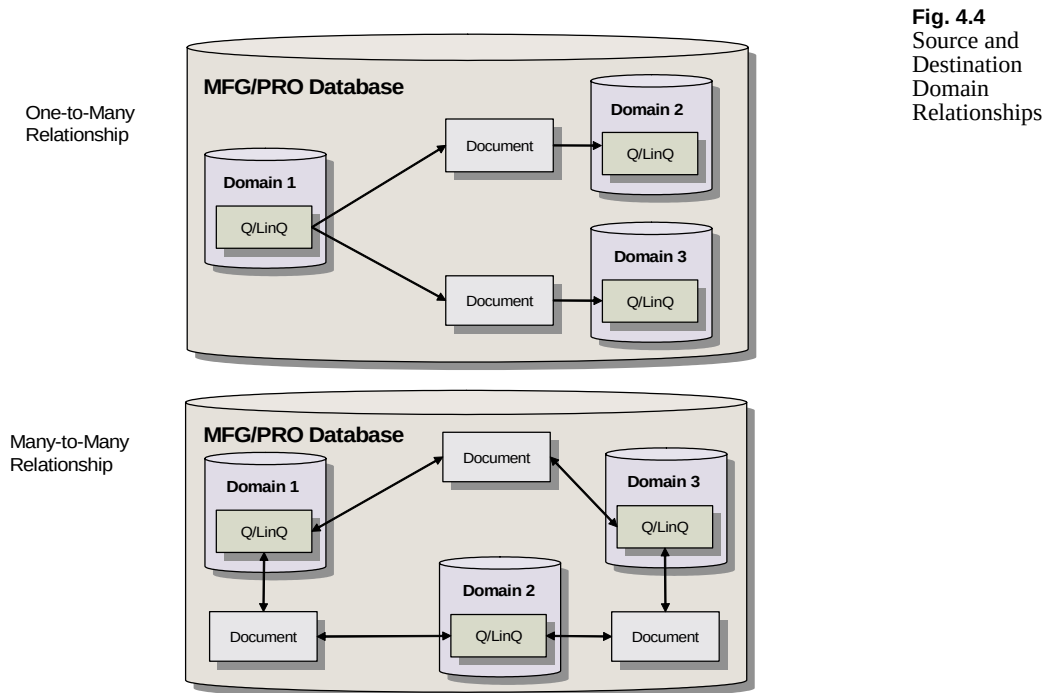
Fig. 4.3
Data Flow Among
Domains Using
Forwarding



When a table included in a synchronization profile is updated in a source domain, Q/LinQ publishes the data to an export document and places it directly in the import queue of the destination domain. Q/LinQ then maps and processes the data in the destination domain.

Note In this scenario, one installed instance of Q/LinQ manages documents in all domains without establishing a communications link between them. In addition, the number of steps is reduced since the sending and receiving steps used between databases are not required.

Figure 4.4 illustrates the relationships among domains in a single database where Q/LinQ forwarding is used.



Note Figure 4.4 illustrates relationships only; one instance of Q/LinQ in the database manages all these relationships.

Source and destination domains can be in one-to-one, one-to-many, and many-to-many relationships. A source domain can synchronize different tables with different destination domains or different fields from the same table with different destination domains.

Note When synchronizing among domains using Q/LinQ forwarding, destinations lists cannot be used. Instead you can use Export/Import Specification Copy (36.8.1.4) to streamline the setup of similar specifications.

See “Copy Import and Export Specifications” on page 160.

Synchronization Documents

The records in export documents are published in Q/LinQ triplet format from data captured and filtered as specified by synchronization profiles. Each data field is represented with up to three character tokens:

[<context>]<name>=<value>

Where the token definitions are:

<context> An optional qualifier used to identify the table name
 <name> The name of the MFG/PRO field
 <value> The value of the field expressed as an ASCII string

Each triplet is terminated by an end-of-line (carriage return or line feed) or a delimiter defined in the Data Mapping Parameters frame of Register External Applications (36.8.1.1), Export Specification Maintenance (36.8.1.2), or Import Specification Maintenance (36.8.1.3). The default delimiter is the pipe symbol (|).

Specifying Actions

Each document also includes a field indicating the type of action it represents:

action=A Add the data to the destination domain.
 action=C Change the data in the destination domain.
 action=D Delete the data from the destination domain.

For change actions, only net changes to a record are exported. These are the fields that have changed since the last maintenance transaction.

Example The published document includes this line when only the order quantity for the item has changed:

[pt_mstr]|action=C|pt_part=10-100-A|pt_ord_qty=120

Identifying Records Across Databases

Some tables that can be synchronized lack a meaningful unique key for identifying records between databases. For example, the price list detail table (pid_det) uses a database sequence (pid_list_id) in its unique key and database sequences are not meaningful across MFG/PRO databases.

When a table lacks a meaningful unique key, the published document includes key information from a related master record. With this combination of master record data and detail record data, the destination database can identify the appropriate record to update.

Example This document for making price list detail changes includes unique identifying information from the price list master record:

```
[pi_mstr]|pi_list=test01|pi_list_id=100051|pi_cs_type=9|
pi_cs_code=qadall|pi_part_type=6|pi_part_code=qadall|
pi_curr=USD|pi_um=EA|pi_start=01/04/00

[pid_det]|action=C|pid_amt=50|pid_list_id=100051|
pid_qty=5
```

Note Q/LinQ processes this data the same way regardless of whether it is being published to another database or another domain within the current database. This is true even though the sequence number would be meaningful in the context of a single database.

Moving Data Between Domains

You can use any of the following Q/LinQ-supported methods when synchronizing data between domains within a single database or in connected databases:

- Intra-database forwarding (within a single database only)
- Q/LinQ-to-Q/LinQ Adapter (stream API)
- Messaging API
- File write/read

► See “Set Up Communication Between Databases” on page 147 for details.

The recommended method for communicating synchronization data between domains is the Q/LinQ provided adapter, `qqqq2qq.p`, which is implemented using the Q/LinQ stream API. When all domains exist within a single database, using `qqqq2qq.p` streamlines setup, since you do not need to execute either the send or receive step; documents are published directly to the import queue of destination domains using Q/LinQ document forwarding capabilities.

When domains exist in separate databases, using this `qqqq2qq.p` adapter ensures a robust connection and also reduces the amount of setup required. With this adapter, sending and receiving documents is combined

into one step. Without it, you must always execute a separate send and receive step to accommodate the message-oriented middleware that mediates the communication.

The Q/LinQ-to-Q/LinQ adapter can also be used to communicate between domains located in the same database, in place of intra-database forwarding. In this case, changes to data in the source domain are logged as Q/LinQ export documents, then re-imported into the destination domains using Q/LinQ send or receive functions. This approach adds run-time steps that are not required with intra-database forwarding, but has significant advantages related to performance and logging:

- **Performance.** With intra-database forwarding, Q/LinQ import documents are written into all the receiving domains when the MFG/PRO user updates the data in the source domain. When there are many receiving domains, updates will take longer to complete.

In one-to-many scenarios where a single source domain must synchronize with many receiving domains within its database, intra-database forwarding could adversely affect MFG/PRO end-user performance in the source domain.

With the Q/LinQ-to-Q/LinQ adapter, you can create a single destination list for the receiving domains. With lists, only a single export document is logged for all of receiving domains when the data is updated in the source domain.

- **Logging.** The Q/LinQ-to-Q/LinQ adapter provides a built-in audit trail of the data exported from each domain as well as the data imported into each domain. With intra-database forwarding, only import logs are written.

Note While it is possible to configure Q/LinQ to use file write/read to communicate between domains, this is not recommended.

For file write/read, users must provide their own batch control procedures for data integrity and loss protection. It is possible to read files continuously into Q/LinQ with a user-written polling procedure.

Table 4.1 summarizes the differences between the requirements for different communication approaches to data synchronization.

Communication Approach	Register as External Application	Use Destination Lists	Send from Source	Receive into Destination	Logging
Intra-Database Forwarding	No	No	No	No	Destination domain only
Q/LinQ-to-Q/LinQ Adapter (qqqq2qq.p) of Stream API	Yes	Yes	Either send or receive	Either send or receive	Source and destination domains
Messaging API (qqmsgapi.p)	Yes	Yes	Yes	Yes	Source and destination domains
File Write/Read	No	No	Yes	Yes	Source and destination domains

Table 4.1
Communication Approaches

Data Mapping

In the source MFG/PRO domain, Q/LinQ creates synchronization export documents in triplet format. In the destination MFG/PRO domain, Q/LinQ uses table-specific mapping programs to map the data to CIM format.

If site codes are not the same in different domains, Q/LinQ checks any values for pt_site defined in Code Mapping Maintenance (36.8.1.20) and maps them appropriately.

For the programs that update synchronized tables, Q/LinQ can process batch delete transactions through the CIM interface. The batch delete functionality is enabled only when the programs are accessed through a batch process; it is not enabled when the programs are used interactively. The one-character, unlabeled batch delete field is not visible to users, requires no changes to the user interface, and does not break existing CIM data files. Q/LinQ captures the delete action and the response to the Please Confirm Delete prompt. Use Ctrl+F in any of these programs to confirm that batch delete is enabled.

For more information on batch delete, see the chapter on the CIM Interface in *User Guide Volume 9: Manager Functions*.

♦ See Table 4.3, “Synchronization Data Mapping Programs,” on page 159.

♦ See “Create Optional Code Mappings” on page 149.

♦ See Table 4.2 on page 126.

Tables to Synchronize

Table 4.2 lists the database tables that can be updated using data synchronization features of Q/LinQ. Also listed are the MFG/PRO programs that are typically used to update the tables interactively.

The column labeled Required Table lists tables associated with the table being synchronized. These tables contain data that is validated during the update of the first table. If the data does not exist in the target domain, the synchronization will fail. You should ensure that data in prerequisite tables is also synchronized.

Table 4.2
Tables to
Synchronize

Table	Table Description	Menu Label	Program	Req. Table
ac_mstr	Account Master	Account Code Maintenance	glacmt.p	code_mstr cu_mstr al_mstr fm_mstr
acdf_mstr	Account Default Master	Currency Account Maintenance	mccuacmt.p	cu_mstr ac_mstr al_mstr sb_mstr cc_mstr
an_mstr	Analysis Code Master	Analysis Code Maintenance	ppacmt.p	anl_det ans_det
anl_det	Analysis Code Link Detail	Analysis Code Link Maint	ppacln.p	an_mstr ans_det
ans_det	Analysis Code Selection Detail	Analysis Code Select Maint	ppacrl.p	an_mstr anl_det
bom_mstr	Product Structure Bill of Material	Product Structure Code Maint	bmmamt.p	
cc_mstr cr_mstr	Cost Center Master Code Range Master	Cost Center Code Maintenance	glccmt.p	ac_mstr al_mstr sb_mstr
cd_det	Master Comments	Master Comment Maintenance	gpcmmt.p	lng_mstr

Table 4.2 — *Tables to Synchronize* — (Page 1 of 5)

Table	Table Description	Menu Label	Program	Req. Table
cm_mstr ad_mstr ls_mstr	Customer Master Address Master Address List Master	Customer Maintenance	adcsmt.p	code_mstr ctry_mstr sp_mstr ac_mstr al_mstr sb_mstr cc_mstr cu_mstr si_mstr lng_mstr pi_mstr txz_mstr ct_mstr fr_mstr ft_mstr csbd_det
cm_mstr ad_mstr ls_mstr	Customer Master Address Master Address List Master	Customer Ship-To Maintenance	adstmt.p	code_mstr ctry_mstr lng_mstr txz_mstr
code_mstr	Generalized Codes Master	Generalized Codes Maintenance	mgcodemt.p	
cp_mstr	Customer Item Master	Customer Item Maintenance	ppcpmt.p	cm_mstr ad_mstr pt_mstr
cs_mstr	Cost Set Master	Cost Set Maintenance	csmsmt.p	
cu_mstr	Currency Master	Currency Maintenance	mccumt.p	
dpt_mstr	Department Master	Department Maintenance	rwdpmt.p	ac_mstr al_mstr sb_mstr cc_mstr
en_mstr	Entity Master	Entity Code Maintenance	glenmt.p	cu_mstr
exr_rate	Exchange Rate	Exchange Rate Maintenance	mcexrmt.p	cu_mstr
fcs_sum	Forecast Summary	Forecast Maintenance	fcfsmt01.p	pt_mstr si_mstr
glc_cal	General Ledger Calendar	GL Calendar Maintenance	glcalmt.p	glcalmt.p

Table 4.2 — Tables to Synchronize — (Page 2 of 5)

Table	Table Description	Menu Label	Program	Req. Table
is_mstr isd_det	Inventory Status Master Inventory Status Detail	Inventory Status Code Maint	icstmt.p	code_mstr
ls_mstr	Address List Master	Address List Type Maintenance	adlsmt.p	ad_mstr
pc_mstr	Price List Master – Purchasing	Price List Maintenance	pppcmt.p	cu_mstr pl_mstr pt_mstr um_mstr
pi_mstr pid_det	Price List Master Price List Detail – Sales	Price List Maintenance	pppimt.p	an_mstr cu_mstr um_mstr ac_mstr al_mstr sb_mstr cc_mstr pj_mstr
pl_mstr	Product Line Master	Product Line Maintenance	ppplmt.p	code_mstr ac_mstr al_mstr sb_mstr cc_mstr
ps_mstr	Product Structure Master	Product Structure Maintenance	bmpsmt.p	pt_mstr code_mstr
pt_mstr	Item Master	Item Master Maintenance	ppptmt.p	code_mstr um_mstr pl_mstr pcl_mstr loc_mstr alm_mstr is_mstr csim_mstr vd_mstr si_mstr ssm_mstr ssd_det ro_det bom_mstr cs_mstr

Table 4.2 — Tables to Synchronize — (Page 3 of 5)

Table	Table Description	Menu Label	Program	Req. Table
ro_det	Routing Operation Detail	Routing Operation Maintenance	rwromt.p	wc_mstr code_mstr vd_mstr pt_mstr
sb_mstr cr_mstr	Sub-Account Master Code Range Master	Sub-Account Code Maintenance	glsbmt.p	ac_mstr al_mstr
si_mstr	Site Master	Site Maintenance	icsimt.p	en_mstr is_mstr vd_mstr ac_mstr al_mstr sb_mstr cc_mstr
spt_det sct_det	Cost Simulation Item Detail Cost Simulation Total Detail	Item-Element Cost Batch Load	ppcsbtd.p	pt_mstr si_mstr cs_mstr sc_mstr
um_mstr	Alternate Unit of Measure Master	Unit of Measure Maintenance	pppummt.p	pt_mstr
vd_mstr ad_mstr ls_mstr	Supplier Master Address Master Address List Master	Supplier Maintenance	advnmt.p	code_mstr ctry_mstr ac_mstr al_mstr sb_mstr cc_mstr bk_mstr cu_mstr lng_mstr pc_mstr ct_mstr txz_mstr csbd_det
vd_mstr ad_mstr ls_mstr	Supplier Master Address Master Address List Master	Supplier Remit-To Maintenance	adrtmt.p	code_mstr ctry_mstr txz_mstr

Table 4.2 — Tables to Synchronize — (Page 4 of 5)

Table	Table Description	Menu Label	Program	Req. Table
vp_mstr	Supplier Item Master	Supplier Item Maintenance	ppvpm.t.p	pt_mstr vd_mstr ad_mstr um_mstr cu_mstr pc_mstr
wc_mstr	Work Center Master	Work Center Maintenance	rwwcmt.p	dpt_mstr

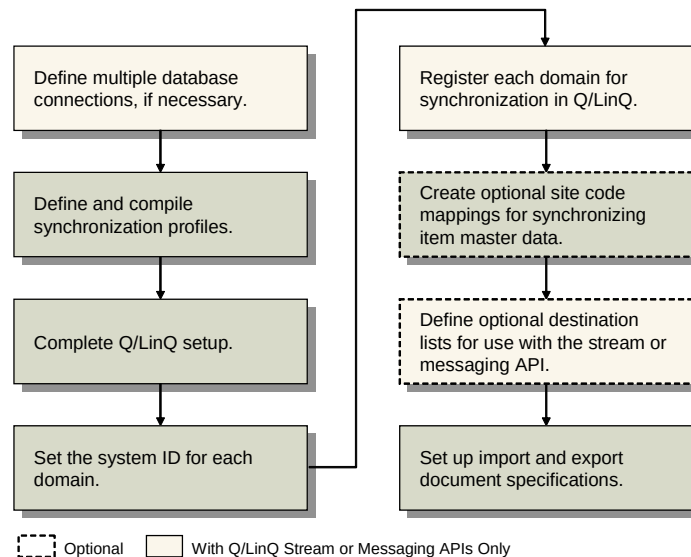
Table 4.2 — Tables to Synchronize — (Page 5 of 5)

Setting Up Synchronization

A number of setup steps are required to enable synchronization among multiple MFG/PRO domains. The steps vary depending on whether you are setting up synchronization between domains using Q/LinQ intra-database forwarding or using the Q/LinQ stream or messaging API. Setting up synchronization through intra-database forwarding requires fewer steps.

Figure 4.5 illustrates a typical work flow for setting up synchronization. See Figure 4.24 on page 162 for the processing work flow.

Fig. 4.5
Synchronization
Setup Flow



In Figure 4.5, the steps with lighter shading are not required when setting up synchronization for domains within a single database using intra-database forwarding.

- 1 Define database connections for all MFG/PRO databases participating in the synchronization using Database Connection Maintenance (36.6.1). This information lets Q/LinQ connect to domains in the other databases when required.
 - 2 Define and compile synchronization profiles. These can be shared by all domains in a database. ▶ See page 132.
 - 3 Complete the Q/LinQ setup. Complete information about setting up Q/LinQ can be found in *External Interface Guide: Q/LinQ* and *Technical Reference: Q/LinQ*.
 - 4 Set up system IDs for each domain in each database involved in synchronization. The system ID should normally be the same as the domain code. ▶ See page 143.
 - 5 To synchronize between databases, register each external MFG/PRO domain in each domain that is involved in synchronization. This step is not needed if you are synchronizing data among domains in a single database using intra-database forwarding. However, if you use Q/LinQ APIs to synchronize data among domains in a single database, you must complete this step. ▶ See page 144.
 - 6 Optionally define code mappings for sites in different domains. ▶ See page 149.
 - 7 Optionally define destination lists in the source domain when the Q/LinQ stream or messaging API is used to link the domains. ▶ See page 150.
 - 8 Create export specifications in source domains for outbound synchronization documents. ▶ See page 154.
 - 9 Create import specifications in destination domains for inbound synchronization documents. ▶ See page 157.
- Note** You can streamline steps 8 and 9 by creating template specifications and copying them. ▶ See “Copy Import and Export Specifications” on page 160.

Review Tables and Fields for Synchronization

Sync Table–Field Maintenance (36.8.22.3) is populated with the names of the tables and fields that can be synchronized during database initialization. In most cases, the valid fields are those that can be updated directly by MFG/PRO users through standard MFG/PRO menu procedures.

If you have modified MFG/PRO maintenance programs to display additional fields for update (for example, user-reserved table fields), you can use this procedure to make the new fields eligible for inclusion in synchronization profiles.

Important You should use security functions to limit access to this program. Incorrect entries can result in runtime Progress errors.

When you define a profile, Synchronization Profile Maintenance (36.8.22.1) validates tables and fields proposed for the profile against those in Sync Table–Field Maintenance.

To prepare for defining profiles, use Sync Table–Field Browse (36.8.22.4) to review the fields that can be synchronized from each table that can be synchronized.

Define Synchronization Profiles

Synchronization profiles specify which data—records and fields—to synchronize between domains and which types of data change—add, change, delete—to synchronize.

Synchronization profiles are not domain specific. This lets you share profiles among domains in a database. For example, if you need to keep the item master synchronized among three domains, you can use the same profile for each. If you do not want to share profiles, establish a naming convention to distinguish them.

Since profiles are defined without reference to a destination, they can also be used to implement synchronization with multiple destination databases.

This section covers general profile setup as well as setup for tables with dependencies.

Use Synchronization Profile Maintenance (36.8.22.1) to define profiles.
 Use Synchronization Profile Inquiry (36.8.22.2) to review the contents of synchronization profiles.

Default Profiles

To simplify profile setup, a set of default profiles is loaded during system initialization. A profile exists for each table that can be synchronized. These profiles support the synchronization of all records and eligible fields.

You can use these profiles they way they are; however, if you want to filter data based on some criteria, you can modify them to meet your requirements or create your own.

Note Even if you use the profiles delivered by QAD, they must be compiled.

◆ See “Compiling Profiles” on page 136.

These profiles have the same name as their associated table. For example, the profile for synchronizing item master data is pt_mstr.

General Profile Setup

Synchronization profiles contain the following:

- The name of the MFG/PRO table with data to be synchronized. Each profile can specify only one table.
- Settings indicating which events (add, change, delete) create a synchronization document.
- Selection criteria specifying which records from the table should be synchronized. This is the filtering criteria.
- The fields in the specified table whose value will be included in the synchronization document. This is the payload.

◆ See Table 4.2 on page 126.

Fig. 4.6
Synchronization
Profile
Maintenance
(36.8.22.1)

Synchronization Profile Maint All Domains (USD)

Synchronization Profile ID: acdf_mstr_curr

Description: Currency Account Default Master Profile

Table Name: acdf_mstr

Export Add: ☒

Export Change: ☒

Export Delete: ☒

Format As Change: ☐

Format As Change: ☐

Selection Criteria

acdf_module = "CU"

Sync Profile ID. Enter a unique identifier for the synchronization profile.

Description. Enter up to 40 characters describing the synchronization profile.

Table Name. Enter the name of the table with fields to be included in the synchronization document. This table must be listed in Sync Table–Field Maintenance.

Export Add. Enter Yes to export data records that now match the selection criteria of the synchronization profile where previously they did not match the criteria. A record may be new or it may now match the selection criteria because its value has been updated.

Format as Change. Enter Yes to format records selected by Export Add as changes when exporting. This field should be Yes only when the destination domains have already set up all possible records in advance. Set this field to Yes to avoid sending an add-record instruction to a domain where the record already exists.

Export Change. Enter Yes to export data records that are updated. This applies to records that previously met and still meet the selection criteria of the synchronization profile.

Export Delete. Enter Yes to export a delete instruction for a record with a value that no longer meets the selection criteria of the synchronization profile. The record may continue to exist in the source domain but its data is no longer exported for synchronization.

Tip
You cannot change this value after it has been defined.

Format as Change. Enter Yes to format records selected by Export Delete as changes when exporting. Set this field to Yes when records cannot be deleted from the destination domain but record status must change, such as an item changing from an active to an obsolete state.

Selection Criteria. Enter the legal Progress 4GL syntax for selecting records to synchronize. Use this field to describe a subset of data records from the synchronization profile's database table, such as only items with an active status or only items in product line 100. The criteria is validated, interpreted, and processed as a Progress 4GL WHERE clause.

Use Progress functions or operators in any combination containing one or more levels of parenthesized expressions if necessary. Use only logical expressions; do not use IF, ELSE, WHERE, or other reserved words.

References can be made only to the table associated with the current synchronization profile, except inside CAN-FIND function invocations, which can reference other tables. The system compiles the entered expression and returns any Progress error messages as warning conditions to the user.

Blank causes all records in the table to be subject to synchronization.

The screenshot shows a window titled "Synchronization Profile Maint" with a subtitle "All Domains (USD)". It contains two main sections: "Field Payload Detail" and "Field Payload Maintenance".

Field Payload Detail

Field Name	Label	Seq	Add	Chg/Del
acdf_key1	ACDF_KEY1	1	☒	☒
acdf_type	ACDF_TYPE	2	☒	☒
acdf_acct	ACDF_ACCT	3	☒	☐
acdf_sub	ACDF_SUB	4	☐	☐
acdf_cc	ACDF_CC	5	☐	☐

Field Payload Maintenance

Field Name	Label	Seq	Add	Chg/Del
acdf_key1	ACDF_KEY1	1	☒	☒

At the bottom right of the maintenance section are three buttons: a red 'X' (cancel), a left arrow, and a right arrow.

Fig. 4.7
Synchronization
Profile
Maintenance, Field
Payload Frames

The Field Payload Detail frame displays current settings for each field in the table.

Use the Field Payload Maintenance frame to add fields to the profile payload and modify or delete existing fields in the payload.

Field Name. Select the field to be added to, modified, or deleted from the profile payload.

Sequence. Enter the sequence of the field in the profile payload. This field does not affect processing. Use it to order the fields for convenience.

If a sequence number is not assigned or if a number is assigned that is greater than the number of fields in the profile, Q/LinQ assigns the next available number to the field. As you assign fields different numbers, Q/LinQ closes gaps in the sequence and renumbers all fields so that the highest sequence number is always the number of fields in the profile payload.

Required on Add. Enter Yes to always export the field for add actions, and to delay the publishing of the record until the field has been populated with a non-empty value. Use this to export key or other fields required to create a new record in the destination domains.

Example Always export product line (pt_prod_line) when adding item master (pt_mstr) records, and do not publish the new pt_mstr record until its product line has been assigned. Although it is not a pt_mstr key, a new record requires a value for the pt_prod_line field.

Require on Change or Delete. Enter Yes to always export the field for change or delete actions. Use this to export key fields used for locating records in the destination domain.

Example Always export item number (pt_part) when modifying item master (pt_mstr) records because it is the unique key for the pt_mstr table.

Compiling Profiles

After you add the fields you want included in the payload of the synchronization profile, leave the Field Payload Detail frame by pressing End. This causes Progress r-code to be automatically generated and

compiled from the synchronization profile and stored in the Q/LinQ archive directory, as established in the Q/LinQ initialization file `qqapi.ini`.

If any compile errors occur—typically due to invalid selection criteria—Progress errors display as warning messages. The profile cannot be used until the r-code is compiled successfully from Synchronization Profile Maintenance.

Important Predefined synchronization profiles provided by QAD do not work until you press End from the Field Payload Detail frame of Synchronization Profile Maintenance for each of the profiles. This must be done to properly compile the r-code even when you do not modify the content of the profiles.

Setting Up General Header-Detail Tables

Related tables such as those with header-detail or parent-child relationships must be updated in the destination domain at the same time. For example, synchronizing analysis code link detail (`anl_det`) without synchronizing analysis codes (`an_mstr`) would not be meaningful. And synchronizing only analysis code link detail would not provide sufficient information for the destination domain to use the data.

Use this setup for synchronizing related tables:

- Use Synchronization Profile Maintenance to set up synchronization profiles with matching selection criteria for the header (parent) and detail (child) tables. For example:

Table	Selection Criteria in the Synchronization Profile
<code>an_mstr</code>	<code>an_code >= "1000", an_code <= "5000"</code>
<code>anl_det</code>	<code>anl_code >= "1000", anl_code <= "5000"</code>

- In the source domain, use Export Specification Maintenance to create export specification records that associate the header and detail synchronization profiles with the destination domain.
- In the destination domain, use Import Specification Maintenance to set up import specification records with document types that match those in the header and detail export specification records.

Setting Up Addresses

You can synchronize data for the following types of MFG/PRO addresses:

- Customer
- Customer ship-to
- Supplier
- Supplier remit-to

Because of the way address data is stored in the MFG/PRO database, updating one of these records can affect up to three tables:

- The table for the specific address type (cm_mstr, vd_mstr)
- The table for general address information (ad_mstr)
- The table that stores system and user-defined address list types (ls_mstr)

Tip
Cross-references between ad_mstr records and cm_mstr records are stored in ls_mstr.

For each destination domain, ad_mstr and ls_mstr records are synchronized only when they are associated with customer or supplier records that are set up for synchronization.

◆ See “Address List Type Table Setup” on page 140.

Note You can choose to synchronize address list data, but only for types that are not system generated.

To streamline synchronization, it is best to have one address profile for each type of synchronized address: supplier, customer, ship-to, and remit-to. This provides more flexibility in controlling the events that require synchronization for each address type and also the fields that need to be synchronized.

Use the guidelines in the following sections for setting up address synchronization profiles in source domains. In each case, after setting up profiles, complete these steps:

- 1 In the source domain, use Export Specification Maintenance to create export specification records that associate the profiles with the proper destination domain.
- 2 In the destination domain, use Import Specification Maintenance to set up import specification records with document types that match those in the export specification records.

Note You can also create template specifications and use Export/Import Specification Copy (36.8.1.4) to quickly create similar records in multiple domains.

◆ See “Copy Import and Export Specifications” on page 160.

Customer and Address Master Table Setup

Set up synchronization profiles for the cm_mstr and ad_mstr tables. The selection criteria need not be the same since Q/LinQ automatically checks for association between customer and address records.

For customers, it is recommended that the following selection criteria be used for the ad_mstr profile:

`ad_ref = "" and ad_type = "customer"`

For customer ship-to addresses, use the following selection criteria for the ad_mstr profile:

`ad_ref <> ""`

For customer records, you should also set the Required on Add field to Yes for the cm_site field in the cm_mstr payload. This prevents the creation of source documents with incomplete information that might fail to be loaded in the receiving domain.

Supplier and Address Master Table Setup

Set up synchronization profiles for the vd_mstr and ad_mstr tables. The selection criteria need not be the same since Q/LinQ automatically checks for association between supplier and address records.

For suppliers, it is recommended that the following selection criteria be used for the ad_mstr profile:

`ad_ref = "" and ad_type = "supplier"`

For supplier remit-to addresses, use the following selection criteria for the ad_mstr profile:

`ad_ref = "" and ad_type = "remit-to"`

For suppliers, you should also set the Required on Add field to Yes for the vd_curr field in the vd_mstr payload. This prevents the creation of source documents with incomplete information that might fail to be loaded in the receiving domain.

Address List Type Table Setup

Only list types that have been assigned by users can be synchronized directly. System-assigned address list types are not synchronized since these list type are created automatically when the associated address records are created.

Note System-assigned list types include slsprsn, company, customer, enduser, ship-to, supplier, remit-to, dock, c/s_bank, our_bank, po-ship, carrier, and engineer.

Use this setup for synchronizing address list type records:

- 1 Set up synchronization profiles for the cm_mstr, vd_mstr, ad_mstr (ship-to, remit-to), and ls_mstr tables.
- 2 In the source domain, use Export Specification Maintenance to create export specification records that associate the ls_mstr, cm_mstr, vd_mstr, and ad_mstr synchronization profiles with the destination domain.
- 3 In the destination domain, use Import Specification Maintenance to set up import specification records with the document types that match those in the ls_mstr, cm_mstr, vd_mstr, and ad_mstr export specification records

Setting Up Bill of Material Profiles

You can synchronize only bill-of-material (BOM) records (bom_mstr) that are created, modified, or deleted using Product Structure Code Maintenance (13.1). Other options for creating bom_mstr records in the following programs are not supported at this time:

- Service BOM Code Maintenance (11.19.1)
- Formula Code Maintenance (15.1)

Use this setup for synchronizing BOM records:

- 1 Set up synchronization profiles for the bom_mstr table using the following selection criteria:
 bom_formula = no and bom_fsm_type = "" and
 bom_batch = 0.0

- 2 In the source domain, use Export Specification Maintenance to create export specification records that associate the bom_mstr synchronization profiles with the destination domain.
- 3 In the destination domain, use Import Specification Maintenance to set up import specification records with the document types that match those in the bom_mstr export specification records.

Setting Up Product Structure Profiles

You can synchronize only product structure records (ps_mstr) that are created, modified, or deleted using Product Structure Maintenance (13.5). Other options for creating ps_mstr records in the following programs are not supported at this time:

- Configured Structure Maintenance (8.1)
- Service Structure Maintenance (11.19.5)
- Alternate Structure Maintenance (13.15)
- Co/By-Product Maintenance (13.22.1, 15.12.1)
- Formula Maintenance (15.5)
- Process/Formula Maintenance (15.18)

Use this setup for synchronizing product structure records:

- 1 Set up synchronization profiles for the ps_mstr table using the following selection criteria:
`ps_ps_code <> "J" and ps_ps_code <> "A" and
ps_qty_type = ""`
- 2 In the source domain, use Export Specification Maintenance to create export specification records that associate the ps_mstr synchronization profiles with the destination domain.
- 3 In the destination domain, use Import Specification Maintenance to set up import specification records with the document types that match those in the ps_mstr export specification records.

Setting Up Routing Detail Profiles

You can synchronize only routing records (ro_det) that are created, modified, or deleted using Routing Maintenance (14.13.1). Other options for creating ro_det records in the following programs are not supported at this time:

- Service Routing Maintenance (11.19.17)
- Routing Maintenance—Rate Based (14.13.2)
- Formula Maintenance (15.13)
- Process/Formula Maintenance (15.18)

Use this setup for synchronizing routing records:

- 1 Set up synchronization profiles for the ro_det table using the following selection criteria:
ro_fsm_type = ""
- 2 In the source domain, use Export Specification Maintenance to create export specification records that associate the ro_det synchronization profiles with the destination domain.
- 3 In the destination domain, use Import Specification Maintenance to set up import specification records with the document types that match those in the ro_det export specification records.

Complete Q/LinQ Setup

♦ See *External Interface Guide: Q/LinQ*.

Install and set up Q/LinQ for each MFG/PRO database that will export data to or import data from other MFG/PRO databases for data synchronization.

Note Only one instance of Q/LinQ is required if you are going to synchronize data between domains in a single database.

♦ See *User Guide Volume 9: Manager Functions* for details on security.

You should limit access to most Q/LinQ programs—including the data synchronization programs—to administrators. Use Menu Security Maintenance (36.3.10) to set menu-level security for the programs in Table 1.7 on page 24. This limited access is especially important for Sync Table—Field Maintenance (36.8.22.3), which identifies the tables and fields that can be synchronized. This table is populated during installation and should not be modified.

Important Do not use Sync Table–Field Maintenance to add other tables or fields since these are not supported by the software and lead to runtime Progress errors.

Set Up System IDs for Domains

The system ID defined in Q/LinQ Control (36.8.24) identifies the source MFG/PRO system on exported documents. This ID is typically set to the domain code. In a multiple-domain environment, this ensures that you can easily and consistently identify where documents originated.

When an import or export specification references a system ID in the current database that is not registered with Q/LinQ as an external application, Q/LinQ recognizes that synchronization is taking place with a domain in the current database, and copies the data across domains using intra-database forwarding.

When Q/LinQ Control is first accessed, system ID defaults to the current working domain.

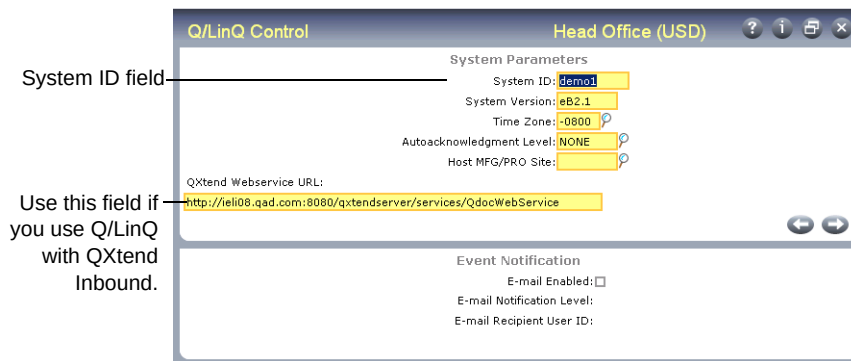


Fig. 4.8
Q/LinQ Control
(36.8.24), System
ID Field

Q/LinQ validates that the system ID is unique within the database and is not the same as any other application ID defined in Register External Application (36.8.1.1).

If you have installed QXtend Inbound, specify the URL that identifies the QXtend server in your system (maximum 70 characters). The system uses this URL to locate the server when the import specification associated with a document indicates that it should be processed through QXtend.

► See *Technical Reference: QXtend Inbound* for details.

Register Domains

Important This step is required only when you are synchronizing data with domains using the Q/LinQ-to-Q/LinQ adapter or Q/LinQ messaging API. It is not needed for intra-database forwarding.

▶ See *External Interface Guide: Q/LinQ* for additional details.

In each source MFG/PRO domain, register each destination MFG/PRO domain as a Q/LinQ external application in Register External Application (36.8.1.1). Accept the Q/LinQ defaults except where noted. You must also create the corresponding registrations in each destination domain by registering each source domain.

The key fields for registering domains are Application ID and Access Code/Path:

- Each application ID identifies a domain in this or an external MFG/PRO database. Set it to the value of system ID in Q/LinQ Control of the referenced domain.
- The Access Code/Path specifies the actual domain code as defined in Domain Maintenance (36.10.1). The system determines the database associated with the domain based on the value defined in Domain Maintenance. If the database is not the current one, database connection parameters are found in Database Connection Maintenance (36.6.1).

▶ See “Domain Maintenance” on page 61.

Note The Q/LinQ system ID is typically the same as the domain code; keeping them the same makes it simpler to identify document ownership.

Application ID Examples

The data you define in Register External Application is domain specific. If more than one domain shares data with another domain, you must complete the database registration tasks in each domain. This ensures that export and import documents are always sent to and received by the correct domain.

The following examples illustrate setting up IDs in different scenarios.

Example 1: Many-to-Many

Three possible combinations exist for three domains in three separate databases (Domain1, Domain2, Domain3) that each exchange data with all of the others. Use the domain system ID values as the application IDs when registering the databases/domains in Q/LinQ.

♦ See Figure 4.2 on page 119.

In this Domain System ID	Register These Application IDs
domain1	domain2, domain3
domain2	domain1, domain3
domain3	domain1, domain2

Example 2: One-to-Many

A configuration of one central domain (domainC) and two peripheral domains in separate databases (domainE and domainW) has only two possible combinations. The sample application IDs and the domains where they must be registered are shown in this table.

♦ See Figure 4.2 on page 119.

In this Domain System ID	Register These Application IDs
domainC	domainE, domainW
domainE	domainC
domainW	domainC

Register IDs

In Register External Application, enter the application ID for a domain in a synchronization relationship. Also enter a name and description for the synchronization represented by the application ID.

In the Select Data Update frame, enter Yes in these fields:

- Interface Control Parameters, to update e-mail settings
- Default Communications Parameters, to set up between-database communication
- Miscellaneous Defaults, to embed document control tags when using the stream or messaging API

Press Go to display the first frame selected for update. After making edits, press Go again to display the next frame selected for update. Press End at any time to return to the main program screen.

Fig. 4.9
Register External
Application
(36.8.1.1)

The screenshot shows a window titled "Register External Application" with a subtitle "Head Office (USD)". The window contains the following information:

- Application ID: Domain2
- Name: European Office
- Version: eB2.1
- Description: Registering Domain2 for Synchronization

Below this information is a section titled "Select Data Update" with the following options, all of which are checked:

- Interface Control Parameters: ☒
- Default Data Mapping Parameters: ☒
- Default Communications Parameters: ☒
- Miscellaneous Defaults: ☒
- Return Codes and Messages: ☒

At the bottom of the "Select Data Update" section are two navigation buttons: a left arrow and a right arrow.

Set E-Mail Notification

The e-mail notification settings default from Q/LinQ Control (36.8.24). Set up application-specific e-mail notification in the Interface Control Parameters frame.

Enter the name and preferred e-mail notification level of the system administrator who is the default recipient of any Q/LinQ-generated e-mail messages about this synchronization relationship.

Press Go to display the next frame selected for update.

Fig. 4.10
Register External
Application,
Interface Control
Parameters

The screenshot shows a window titled "Register External Application" with a subtitle "Head Office (USD)". The window contains the following information:

- Default E-mail User ID:
- E-mail Level:
- Enable/Disable Interface Activity: ☐
- Publish Exports: ☒
- Map Exports: ☒
- Send Exports: ☒
- Receive Imports: ☒
- Map Imports: ☒
- Process Imports: ☒
- Autoacknowledgment Generation: ☐
- Autoacknowledgment Level:
- Document Standard:
- Document Type:
- Document Revision:

At the bottom right of the window are two navigation buttons: a left arrow and a right arrow.

Set Up Communication Between Databases

Synchronization documents can be passed between databases as text files or using one of the communication APIs. The recommended method is using `qqqq2qq.p`, discussed next.

Stream API

Use the synchronization adapter, `qqqq2qq.p`, to exchange data through a direct Q/LinQ-to-Q/LinQ Progress database connection. The Progress two-phase commit feature ensures the data integrity of the transmission.

Note The adapter can create a connection between two Progress databases or two Oracle databases (UNIX only); it cannot create a connection between a Progress database and an Oracle database.

In the Default Communication Parameters frame, enter the code of the domain in the external database in Access Code/Path. Q/LinQ determines the database associated with the domain by looking up the domain record defined in Domain Maintenance (36.10.1). If the database is not the current working database, then database switching is initiated.

Enter the `qqqq2qq.p` adapter name in Stream API Adapter Program.

Enter the code of the domain in the external database

► See *External Interface Guide: Q/LinQ* for a discussion of exchanging documents as text files or with APIs.

Fig. 4.11
Default Communications Parameters: Stream API

Messaging API

The messaging API establishes a direct TCP/IP connection with Q/LinQ in an external MFG/PRO database using a Q/LinQ-specific protocol that is independent of Progress client-server connections. This requires a port for each direction of the connection. This can be two different ports, or you can use the same for both import and export.

Note To use the messaging API, leave the Stream API Adapter Program field blank.

Use these guidelines for entering information in both the export and import fields of the Messaging API Socket Parameters frame:

- If the current database initiates the connection as the active caller, enter the host name or the Internet protocol (IP) address and the port number of the remote host, the listener.
- If the remote database initiates the connection and the current database is the passive listener, no host name, IP address, or port number is required.
- For Q/LinQ Initiates Connection:
 - Enter Yes to have the current database actively request a connection with the external MFG/PRO database on the designated host. This means that the current database is the caller or client for the TCP/IP session.
 - Enter No to have the current database monitor its local socket for a connection request from the external MFG/PRO database. This means that the current database is the listener or server for the TCP/IP session.

Note Q/LinQ only initiates the connection; it does not start or stop any program in the external MFG/PRO application.

As shown in Figure 4.12 and Figure 4.13, for two-way data synchronization, the import and export port designations must be complementary between domain pairs in connected databases.

Fig. 4.12
Communication
Parameters:
Domain 1,
Database 1

Default Communications Parameters		
Access Code/Path:	Domain2	
Stream API Adapter Program:		
Messaging API Socket Parameters		
	Export	Import
IP Address or Host Name:	njsu02	ohsu04
Port Number For Export:	9001	9002
Q/LinQ Initiates Connection:	☒	☐

Register External Application Printers, Inc. (USD)

Default Communications Parameters

Access Code/Path: Domain1

Stream API Adapter Program:

Messaging API Socket Parameters

	Export	Import
IP Address or Host Name:	ohsu04	njsu02
Port Number For Export:	9002	9001
Q/LinQ Initiates Connection:	☐	☒

Fig. 4.13
Communication
Parameters:
Domain 2,
Database 2

Miscellaneous Defaults

In the Miscellaneous Defaults frame, enter Yes in Precede Data with Tags to embed document control tags in front of the actual data when using the stream or messaging API to send documents to external databases. Control tags are always included when sending documents to a file.

See *External Interface Guide: Q/LinQ* for a discussion on document control tags.

Create Optional Code Mappings

For some variables or codes, values used in an external application may differ from those used in MFG/PRO. To accommodate these differences, you can use Code Mapping Maintenance (36.8.1.20) to define mappings used to translate data values when documents are exchanged.

When synchronizing data, one particular case may require the use of code mappings. This is the site field (pt_site) associated with items in Item Master Maintenance (1.4.1). If this field is included in the synchronization profile, it must be mapped to a site value that is valid for the destination domain.

When you create a site, you can create a connection record in all active sites in the current database or connected databases. However, creating connection records is optional; it is possible that a site does not exist in all domains containing data being synchronized.

See "Associating Domains with Sites" on page 65.

To prevent errors during synchronization of item master data, you can create a mapping for the site value in a source domain to a valid site value in the destination domain.

Fig. 4.14
Code Mapping
Maintenance
(36.8.1.20)

The screenshot shows a 'Code Mapping Maintenance' window. The title bar includes 'Head Office (USD)' and standard window controls. The main area is divided into three sections. The top section contains labels for 'Application ID:', 'Document Standard:', 'Document Type:', 'Document Revision:', and 'Trading Partner ID:'. The middle section has 'Field Name: pt_site'. The bottom section has 'Source Value: 10000', 'Target Value: 20000', and 'Description: Site 10000 to 20000 Mapping'. The 'Target Value' and 'Description' fields are highlighted in yellow. At the bottom right are three buttons: a red 'X', a left arrow, and a right arrow.

To create a mapping for the Site field, follow these steps:

- 1 Leave the fields Application ID, Document Standard, Document Type, Document Revision, and Trading Partner ID blank. This ensures that the mapping applies to all synchronization documents.
- 2 Specify pt_site as the Field Name.
- 3 For Source Value, specify a site in the source domain associated with item data to be synchronized.
- 4 For Target Value, specify a valid site in the destination domain.
- 5 Enter an optional description of the mapping.

Define Destination Lists

Important This step applies only when you are synchronizing data between domains using the Q/LinQ-to-Q/LinQ adapter or Q/LinQ messaging API.

Destination lists are lists of application IDs defined in Register External Application that can be used for publishing, sending, and deleting/archiving documents. Destination lists are single level; they cannot be nested. In the context of data synchronization, they can be used to streamline the setup required for communicating with multiple external domains or applications.

Note the following restrictions on destination lists:

- They are used for exporting, but not for importing documents.
- They can be used for communicating between domains in the same or other databases, but not for synchronizing data among domains in a single database using Q/LinQ intra-database forwarding.

Using destination lists is optional, but they can facilitate data synchronization among domains in multiple databases or when there are many domains in a single database. Without them, each trigger or export event sends one document to each target domain. Destination lists let you send each event to a list of domains in this or external MFG/PRO databases. This saves disk space and improves runtime performance because it creates only one copy of the export documents for management and storage rather than one for each destination.

Publishing and sending to destination lists are independent tasks:

- Documents published to an individual domain can be sent to that domain or to any destination list to which the domain belongs.
- Documents published to one list can be sent to individual domains or to another list where only the destinations common to both lists receive the document.

Note Documents can be published and sent to domains that are registered to use the stream or messaging APIs for communication. The messaging API can be used with destination lists for sending documents only on UNIX systems. The stream API can be used with destination lists for sending documents on both UNIX and Windows systems.

Use Destination List Maintenance (36.8.8) to define destination lists.

Destination List Maintenance Head Office (USD)

Destination List ID: Subsidiaries

Description:
Subsidiary databases related to head office

Application ID: Domain2

Effective Date In: 01/12/2004

Effective Date Out:

Fig. 4.15
Destination List
Maintenance
(36.8.8)

Destination List ID. Enter a unique name for the destination list.

The system verifies that this name is not currently used as the Q/LinQ system ID for any domain in the current database. System ID is defined for each domain in Q/LinQ Control. Also, this name cannot be the same as any registered application ID in the current domain.

Description. Enter up to 60 characters describing the destination list.

Application ID. Enter the ID of an application registered in Register External Application. For data synchronization, the application ID is the same as the system ID of the domain.

An error displays if the ID you enter is not registered with Q/LinQ as an external application in the current domain.

Effective Date In. Enter the date when the database's membership in the distribution list becomes effective.

Effective Date Out. Enter the date when the database's membership in the distribution list expires.

Set Up Document Specifications

Use Export Specification Maintenance (36.8.1.2) and Import Specification Maintenance (36.8.1.3) to identify particular documents and to set document-specific parameter values for exporting and importing. For exports, you can define interface control, document content, data mapping parameters, messaging, and miscellaneous parameters. For import, you define interface control, data mapping, and miscellaneous parameters.

Note When the specification is associated with a system ID that is not registered as an external application—indicating a domain within the current database—the frames for updating data mapping, messaging, and miscellaneous parameters for export specifications do not display. These values are not used for synchronizing data among local domains.

When specifications are associated with registered applications, many fields default from the values you specify in Register External Application. These defaults do not exist when creating specifications for use with domains in the same database.

♦ See “Register Domains” on page 144.

For registered applications, you may be able to import and export documents without a specific specification in limited cases. In these cases, the values specified in Register External Application are used as is.

Matching Specifications to Documents

You can use up to five values to define an import or export specification: document standard, document type, document revision, application ID, and trading partner ID. The only required field is the document type. The system uses the following logic to find a specification to apply to a document:

- 1 It looks for one with an exact match for document standard, document type, document revision, application ID, and trading partner ID.
- 2 It looks for one with matching document standard, document type, document revision, application ID, and a blank trading partner ID.
- 3 It looks for one with matching document standard, document type, document revision, and blank application and trading partner IDs.

This lets you set up generic specifications that can apply to all documents of a certain type (and optional standard and revision) regardless of the particular application or trading partner associated with a document.

This can be useful when you set up specifications for synchronizing data among domains in separate databases. You can define a generic specification for a particular table (identified by the document type) and leave the application ID blank. Then copy this record to each affected domain using Export/Import Specification Copy. This lets you quickly set up similar export and import specification records.

◆ See “Copy Import and Export Specifications” on page 160.

Required Specifications

Import specifications are required when:

- A document type must be routed to a specific, non-default MFG/PRO program for processing.
- A document type must be mapped by a specific, non-default mapping procedure or mapping specification.

Export specifications are required when:

- A document type must be associated with a specific synchronization profile.
- A document type must be mapped by a specific, non-default mapping procedure or mapping specification.

Defining specifications for unique export documents supports flexibility in data synchronization. For example, you can:

- Export synchronization events for different tables to different destinations.
- Export synchronization events for different fields in specific tables to different destinations.

Register Export Specifications

Use Export Specification Maintenance to:

- Create an export specification for each synchronization document type to be exported to each domain.
- Associate a synchronization profile with each synchronization document type.
- Optionally associate a synchronization profile with a system ID, registered application, or destination list.

Accept the Q/LinQ defaults except where noted.

Fig. 4.16
Export
Specification
Maintenance
(36.8.1.2)

Export Specification Maint Head Office (USD) ? i [icon] x

Application or List ID: Domain2

Document Standard:

Document Type: pt_mstr

Document Revision:

Trading Partner ID:

Description:

Item Master Export

[X] [←] [→]

Application or Destination List ID. Enter one of the following:

- The system ID of another domain in this database as defined in Q/LinQ Control (36.8.24)
- The ID of a domain in this or an external database as it is defined in Register External Application (36.8.1.1)
- The name of a destination list as defined in Destination List Maintenance (36.8.8)

Leave blank if you want this specification to apply to all documents of a certain type, standard, and revision without regard to the associated application.

Document Standard. Enter a user-defined name such as sync_docs so that synchronization activity and documents can be easily segregated from other Q/LinQ documents and activities. This field is validated against generalized codes defined for field esp_doc_std.

Document Type. Enter a user-defined name for the type of data that is being synchronized. Use names that reflect the type of data, such as pt_part for item numbers, to facilitate browsing, reporting, and tracking specific data elements.

Document Revision and Trading Partner ID can be left blank. If they are used, Document Standard, Document Type, Document Revision, and Trading Partner ID must be a unique combination of values.

Fig. 4.17
Export
Specification
Maintenance,
Interface Control
Parameters

Default E-mail User ID, E-mail Level. Enter data for fields, as needed. For registered application IDs, these fields default from Register External Application.

Publishing Enabled. Enter Yes when the export specification is ready to be used by Q/LinQ. Enter No for Q/LinQ to ignore this specification.

Fig. 4.18

Export
Specification
Maintenance,
Document Content

The screenshot shows a window titled 'Export Specification Maint' with a subtitle 'Head Office (USD)'. The 'Document Content' tab is active. It contains a 'Sync Profile ID' field with the value 'pt_mstr' and a 'Publish on Table Update' checkbox that is checked. There are navigation buttons at the bottom right.

Profile ID. Enter the name of a synchronization profile as it is defined in Synchronization Profile Maintenance (36.8.22.1). Only one profile can be associated with an export specification.

Publish on Table Update. Enter Yes to create export documents for the specified profile whenever a record in the associated table is updated. This is event-driven, automatic data exporting.

For batch-only data synchronization, enter No and use Synchronization Mass Export (36.8.22.8) to create export documents for a specified profile.

Note The following frame displays only when you are setting up export specifications for synchronizing data between databases. If the Application ID specified is a domain system ID, this frame is not needed.

Fig. 4.19

Export
Specification
Maintenance,
Messaging and
Miscellaneous
Parameters

The screenshot shows the 'Messaging and Miscellaneous Parameters' tab. It contains various fields for configuration: 'Queue Published Documents' (checkbox), 'Document Language' (dropdown), 'Source Component' (dropdown), 'Task' (dropdown), 'Source User ID' (dropdown), 'Precede Data With Tags' (checkbox), 'Access Code/Path' (text field with 'Domain2'), 'Quality of Service' (checkbox), 'Acknowledgment Level' (dropdown), 'Sync Scope' (dropdown), 'Priority' (dropdown), 'Security' (dropdown), 'Routing' (dropdown), 'Time To Live' (dropdown), 'Message Ordering' (dropdown), and 'Persistence' (dropdown). Navigation buttons are at the bottom right.

Precede Data with Tags. Enter Yes to embed document control tags in front of the actual data when using the stream or messaging APIs to send documents to external databases. Control tags are always included when sending documents to a file.

Access Code/Path. Specify the name of the domain in the external database to receive messages based on this export specification.

Note If you specified a destination list as the Application ID, any value you specify in this field is ignored. Q/LinQ uses the value specified in Register External Application for each application in the list.

Register Import Specifications

Use Import Specification Maintenance (36.8.1.3) to register each inbound synchronization document type. Accept the Q/LinQ defaults except where noted.

Fig. 4.20
Import
Specification
Maintenance
(36.8.1.3)

Application ID. Enter the name of an external MFG/PRO domain as it is defined in Register External Application (36.8.1.1) or the system ID of another domain within the current database defined in Q/LinQ Control (36.8.24).

Leave blank if you want this specification to apply to all documents of a certain type, standard, and revision without regard to the associated application.

Document Standard. Enter a user-defined name such as sync_docs so that synchronization activity and documents can be easily segregated from other Q/LinQ documents and activities.

This field is validated against codes defined in Generalized Codes Maintenance for field esp_doc_std.

Document Type. Enter a user-defined name for the type of data that is being synchronized. Use names that reflect the type of data, such as pt_part for item numbers, to facilitate browsing, reporting, and tracking specific data elements.

Tip
Destination lists
cannot be used with
import documents.

Document Revision and Trading Partner ID can be left blank. If they are used, Document Standard, Document Type, Document Revision, and Trading Partner ID must be a unique combination of values.

Fig. 4.21
Import
Specification
Maintenance,
Interface Control
Parameters

In the Interface Control Parameters frame, set up incoming processing and e-mail notification parameters.

Default E-mail User ID, E-mail Level. Enter data in these fields as needed or accept the defaults specified for the database in Register External Application.

See Table 4.3 on page 159 for a list of MFG/PRO programs.

MFG/PRO Destination Procedure. Enter the name of the MFG/PRO program to call to process the data from the imported synchronization document as an MFG/PRO transaction.

Process Through User Interface. Enter Yes to invoke the destination procedure through the CIM Interface. Yes is required for synchronization.

Fig. 4.22
Import
Specification
Maintenance, Data
Mapping
Parameters

In the Data Mapping Parameters frame, specify the data mapping procedure from Table 4.3. Select the procedure that represents both the destination procedure and the table for the imported data type.

Table 4.3
Synchronization
Data Mapping
Programs

Destination Procedure	Supported Tables	Mapping Procedure Name
adcsmt.p	ad_mstr	qqadmp.p
	cm_mstr	qqcmmp.p
adlsmt.p	ls_mstr	qqlsmp.p
adrtmt.p	ad_mstr	qqadmp.p
	ls_mstr	qqlsmp.p
adstmt.p	ad_mstr	qqadmp.p
	cm_mstr	qqcmmp.p
advnmt.p	vd_mstr	qqvdm.p
	ad_mstr	qqadmp.p
	ls_mstr	qqlsmp.p
bmmamt.p	bom_mstr	qqbommp.p
bmpsmt.p	ps_mstr	qqpsmt.p
csmsmt.p	cs_mstr	qqcsmp.p
fcfsmt01.p	fcs_sum	qqfcsmp.p
glenmt.p	en_mstr	qqenmp.p
glacmt.p	ac_mstr	qqacmp.p
glcalmt.p	glc_cal	qqglcmp.p
	glcd_det	qqglcdmp.p
glsbmt.p	sb_mstr	qqsbmp.p
	cr_det	qqcrmp.p
glccmt.p	cc_mstr	qqccmp.p
	cr_det	qqcrmp.p
gpcmmt.p	cd_det	qqcdmp.p
icsimt.p	si_mstr	qqsimp.p
icstmt.p	is_mstr	qqismp.p
	isd_det	qqisdmp.p
mccuacmt.p	acdf_mstr	qqacdfmp.p
mccumt.p	cu_mstr	qqcump.p
mcexrmt.p	exr_rate	qqexrmt.p
mgcodemt.p	code_mstr	qqcodemp.p
ppacln.p	anl_det	qqanlmp.p
ppacmt.p	an_mstr	qqanmp.p

Table 4.3 — Synchronization Data Mapping Programs — (Page 1 of 2)

Destination Procedure	Supported Tables	Mapping Procedure Name
ppacrl.p	ans_det	qqansmp.p
ppcpmt.p	cp_mstr	qqcpmp.p
ppplmt.p	pl_mstr	qqplmp.p
pppcmt.p	pc_mstr	qqpcmp.p
pppimpt.p	pi_mstr	qqpimp.p
	pid_det	qqpidmp.p
ppptmt.p	pt_mstr	qqptmp.p
pppummt.p	um_mstr	qqummp.p
ppvpmt.p	vp_mstr	qqvpmp.p
rwdpmt.p	dpt_mstr	qqdptmp.p
rwromt.p	ro_det	qqromp.p
rwwcmt.p	wc_mstr	qqwcmp.p

Table 4.3 — Synchronization Data Mapping Programs — (Page 2 of 2)

Copy Import and Export Specifications

In a multi-domain environment that requires extensive sharing of master data, updates from each domain may need to be propagated to many other domains. Q/LinQ requires similar setup information for each destination domain in each source domain.

To facilitate the creation of similar specifications, you can use Export/Import Spec Copy (36.8.1.4) to copy an export or import specification, updating or creating the destination record.

This program can help you streamline the creation of similar specifications. For example, you can create template records and then make multiple copies of them. This minimizes the number of changes needed to complete setup activities.

This function is especially important in a database that includes multiple domains that need to share master data. To support this synchronization, some setup information for other domains must be maintained in each domain that is going to share data. You can create one source import or export specification for each table to be synchronized and then copy it to the other related domains.

You must first create the source specifications using Export Specification Maintenance and Import Specification Maintenance.

You can select a specification from any domain as the source of the copy. The target specification is created in the user's current working domain. In a multiple-database environment, the source domain can exist in another database. The system automatically switches to that domain to find the source record.

If the destination specification exists, the system displays a warning and prompts you to continue. You can overwrite the existing record with values from the source specification.

Fig. 4.23
Import/Export
Specification Copy
(36.8.1.4)

Choose either Import or Export to indicate the type of specification record to be copied.

Domain. Enter the code identifying the domain associated with the source record to be copied.

You can choose any domain in this database or a connected, remote database. The destination domain defaults to your current working domain and cannot be changed.

Application ID. Enter the ID of the application associated with the source specification to be copied.

This can be the ID of an application registered in Register External Application or the Q/LinQ system ID of a domain as specified in Q/LinQ Control. If you are copying an export specification, it can also be a destination list created in Destination List Maintenance.

To. Enter the ID of the application associated with the specification to be created or updated in the destination domain.

Document Standard, Document Type, Document Revision, Trading Partner ID. Enter values in these fields if required to identify the source specification.

To. Enter values for the destination specification if required. These can be the same as or different than the source specification.

Viewing Specification Lists

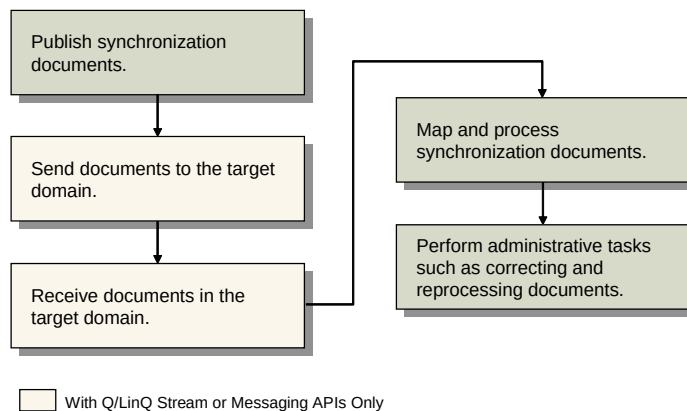
Use Export/Import Specification List (36.8.1.5) to view import or export specifications for a specified document standard, type, and revision combination. You can view records for a specific domain or for all domains. This lets you quickly see the subscription list of senders or receivers associated with a type of document.

Processing Synchronization Documents

After setup tasks are complete, you can begin synchronizing data among multiple, connected MFG/PRO databases or among domains within a database.

Figure 4.24 illustrates a typical work flow for processing synchronization documents.

Fig. 4.24
Synchronization
Processing Flow



When you are synchronizing data among domains in a single database using intra-database forwarding, the processing is simpler:

- 1 Documents are published directly to the import queue of the other domain.
- 2 Documents are mapped according to the import specification in the destination domain and processed to update the relevant tables.

When you are synchronizing data using the stream or messaging APIs between a source domain and domains in the same or connected databases, you must:

- 1 Publish synchronization documents.
- 2 Send the documents to Q/LinQ in the remote database.
- 3 Receive the documents in the remote database.
- 4 Map documents according to the import specification in the destination domain and process them to update the relevant tables.

Note When you are using the Q/LinQ-to-Q/LinQ adapter (qqqq2qq.p), the send and receive step are combined into one since this adapter can directly update the other database without going through a middleware product.

Publishing Documents

Synchronization documents are published automatically through schema triggers or manually through mass export programs.

Synchronization Triggers

With automatic publication, a synchronization document is published each time the table specified in a synchronization profile is updated. This is determined by the setting of Publish on Table Update in Export Specification Maintenance (36.8.1.2).

► See “Publish on Table Update” on page 156.

Mass Document Export

Manual publication is a batch approach to creating synchronization documents. This approach is particularly useful for publishing large numbers of records during initial synchronization of multiple domains or databases.

Use Synchronization Mass Export (36.8.22.8) to publish the documents associated with a selected profile for selected destinations.

Fig. 4.25
Synchronization
Mass Export
(36.8.22.8)

Synchronization Profile ID and To. Enter a range of profile names. For a record from a table specified in a profile to be included in the mass export, any field that is marked as Required for Add must have a value.

Application or Destination List ID and To. Enter a range of destinations to receive the mass-exported documents. When synchronizing in batch between domains in a single database, enter a range of system IDs.

List Documents on Control Report. Enter Yes to include control information about each document on the control report. Enter No to have the report list only the number of document groups selected, processed, sent, containing errors, or skipped.

Control information includes:

- Document ID, group ID, application ID
- Published standard of the document that defines its structure and content after mapping (for example, ANSI X12 or OAGIS)
- Type of document (for example, 850 for ANSI X12 or SYNC SALESORDER for OAGIS BOD)
- Trading partner ID

- Processing stage (published, mapped, sent, or acknowledged)
- Error status (success, warning, failure)

Publish Documents. Enter Yes to publish the documents; enter No to generate the report only.

Sending and Receiving Documents

Important These steps are required only when synchronizing data using the messaging or stream API. When you synchronize data between domains in a single database using intra-database forwarding, Q/LinQ publishes the data directly to the import queue of the destination domain. Only the mapping and processing steps are required (see page 167).

In addition, if you use the Q/LinQ adapter (qqqq2qq.p) for between database communication, you only need to complete the send or the receive step, not both. This is the recommended approach, since it simplifies setup and processing.

If you use the Q/LinQ communication APIs (stream, messaging) or ASCII files to move synchronization documents between MFG/PRO databases, the exchanges can be initiated interactively or through batch scripts.

See these topics in the chapter on “Managing Documents” in *External Interface Guide: Q/LinQ* for details:

- Send Export Document Sessions
- Using Send Export Documents
- Importing from External Applications
- Receiving Import Documents

Exchanging Documents Through APIs

If you do not use the recommended method for exchanging synchronization documents (the Q/LinQ-to-Q/LinQ adapter), you can also exchange documents through the stream and messaging APIs. This approach requires more setup.

♦ See “Messaging API” on page 147.

Important On Windows systems, the messaging API is limited to a single session. If you are using destination lists for sending documents on Windows systems, use the stream API method.

Note When using the messaging API, start the listener process first. It runs as a server waiting for a caller to make contact.

Use Send Export Documents (36.8.7) to export documents to the destination database:

- For Send To, choose Application.
- In Application ID, enter the application ID for the source and destination domain combination as defined in Register External Application. The stream or messaging API parameters are also defined for the application ID in Register External Application.
- In the second frame, specify the ranges defining the documents to export.

Use Receive Import Documents (36.8.9) to import documents from the source database.

- For Import From, choose Application.
- In Application ID, enter the application ID for the source and destination domain combination.

Exchanging Documents Through Files

Exchanging synchronization documents through ASCII files is a manual process. There are no Q/LinQ mechanisms for automatically transferring files between locations (hosts, directories) or for continuously polling directories for files.

Note User-written polling procedures can be created outside of Q/LinQ or using the Q/LinQ stream API to read files continuously into Q/LinQ.

Use Send Export Documents (36.8.7) to export synchronization documents to ASCII files:

- For Send To, select File.
- In File Name, enter the output path.

- In the second frame, specify the application ID for the source and destination domain combination as defined in Register External Application, as well as the ranges defining the documents to export.

Use Receive Import Documents to load ASCII files into the import queue of the domain in the destination database:

- For Import From, select File.
- In Source File Name, enter the path to the ASCII file of synchronization documents.

Mapping and Processing Documents

Use Process Import Documents (36.8.10) to map the synchronization data from the received documents to the appropriate format and to update the destination domain.

In a database with multiple domains, you can use this function to process documents for one domain or for all domains by leaving the Domain field blank. Your current working domain is the default value. If you have centralized Q/LinQ administration, this approach reduces the number of Q/LinQ jobs that need to be started, monitored, and stopped.

Mapping and processing can be initiated interactively or through a batch script. See “Mapping and Processing Import Documents” in *External Interface Guide: Q/LinQ* for details.

To increase processing throughput, run multiple, concurrent sessions of Process Import Documents. It is best to have each session processing different document types and document ranges since concurrent sessions do not preserve the chronological order of synchronization actions.

Performing Q/LinQ Administration

Once Q/LinQ is set up and documents are being processed, Q/LinQ administrators may need to perform a number of routine administration tasks such as:

- Tracking documents
- Correcting and reprocessing documents
- Dumping documents to a text file

- Deleting documents
- Managing Q/LinQ sessions

Tracking Documents

To facilitate document tracking, create unique codes during setup:

◆ See page 154.

- Use Register External Application (36.8.1.1) to specify a unique application ID for each pair of domains in this and an external database that will exchange documents.

◆ See page 157.

- Use Export Specification Maintenance (36.8.1.2) to specify a unique document standard or document type for each synchronization document.

◆ See “Managing Documents” in *External Interface Guide: Q/LinQ*.

With these unique definitions in place, use the standard Q/LinQ tools to monitor and report the status of synchronization activity by database, domain, or document:

- Export/Import Document Query (36.8.16)
- Export/Import Document Report (36.8.17)

Both of these reports let you monitor activity in one or all domains. Your current working domain is the default, but you can specify any other domain or leave the Domain field blank to view activity in all domains.

For documents exported to destination lists, these reports display export log information for each destination.

Correcting and Reprocessing Documents

Occasionally a receiving domain will fail to process a synchronization document as a transaction. This can occur, for example, when all prerequisite codes are not set up in the destination domain.

For CIM documents, use Debug CIM Document (36.8.11) to interactively process the document to more clearly identify the error source.

Note In extreme cases only, use Dump Export/Import Doc for Edit (36.8.13) to manually correct the data inside the destination domain and Reload Edited Export/Import Doc (36.8.14) to reload it for processing.

Dumping Documents to File

Use Dump Export/Import Docs to File (36.8.18) to transfer a range of documents to a text file. In a multiple-domain environment, you can dump documents for one or all domains. Your current working domain is the default, but you can specify any other domain or leave the Domain field blank to dump documents associated with all domains.

This function is most useful for copying existing documents, altering them, then loading the new documents into Q/LinQ using Receive Import Documents (36.8.9).

Fig. 4.26
Dump
Export/Import Docs
to File (36.8.18)

Warning Do not use this procedure to dump documents for transport to external applications. Since it is not a Q/LinQ export process, Q/LinQ cannot track the documents and does not record the dumped documents as sent in the log.

To export documents from MFG/PRO to other applications, use Send Export Documents (36.8.7). To dump documents to archives, use Export/Import Doc Delete/Archive (36.8.23).

You can dump the raw document data or the mapped data. Q/LinQ dumps raw data if mapped data is requested but not present.

The output is a text file of data lines wrapped in header lines. Identifier values in the header describe key document attributes, such as the document type and the source or destination application.

Deleting Documents

◆ See “Deleting or Archiving Documents” in *External Interface Guide: Q/LinQ*.

Since Q/LinQ does not automatically delete completed export or import documents, the number of synchronization documents grows quickly in high-volume environments. Use Export/Import Doc Delete/Archive (36.8.23) to remove completed documents from the export and import queues at least once a day. Cleaning up the queues reclaims storage space and enhances Q/LinQ performance. Export documents can be chosen by destination list as well as by application.

For documents exported to destination lists, Export/Import Doc Delete/Archive deletes export log information for each destination.

In a database with multiple domains, you can use this function to delete and archive documents for one domain or for all domains by leaving the Domain field blank. Your current working domain is the default value. If you have centralized Q/LinQ administration, this approach reduces the number of Q/LinQ jobs that need to be managed.

Managing Sessions

Tracking Sessions

◆ See “Monitoring Q/LinQ Sessions” in *External Interface Guide: Q/LinQ*.

Use Interface Session Monitor (36.8.5) to pause, resume, cancel, or view the status of a session.

For sessions exporting to destination lists, the connections to all databases in the list are controlled through one primary session record. Only the primary session record can be updated directly to pause, resume, cancel, or delete the session. Each discrete connection has its own session master record in the database; these are displayed for inquiry only.

Recovering from Communication Errors

When Q/LinQ encounters a communication error when sending a document to a single application or MFG/PRO database, Q/LinQ attempts to reconnect to the destination database and to resend the document.

Note These kinds of errors would never occur when synchronizing data among domains in a single database.

If a communication error occurs when sending a document to a destination list, Q/LinQ logs the error and goes on to the next destination database rather than attempting to reconnect and resend to the destination database having communication problems. In this way, an error affecting one destination does not delay the delivery of a document to the other destinations.

You can take advantage of the reconnect and resend functionality by publishing a document to a destination list and then sending the document to each of the destination databases one at a time in separate Q/LinQ sessions.

Use the Interface Session Monitor to pause, resume, or cancel the export session at any time. If the session is paused or canceled, a message displays in the Send Export Documents window. If a session is canceled (either through Interface Session Monitor, pressing End, or a system failure), manually delete the session record to release the external application so that other Q/LinQ sessions can connect to it. Delete session records using the delete option in Interface Session Monitor.

Restarting Sessions

After severed communication caused by network problems or user interrupts (Ctrl+C) is restored, the system administrator can restart the MFG/PRO databases. Any documents that were being sent or received at the time of the communication loss remain intact in their source database. Each document has an error status indicating that the sending process was interrupted. The documents can be resent once communication is restored and the databases are restarted.

◆ See “Starting and Restarting Q/LinQ” in *External Interface Guide: Q/LinQ*.

Chapter 5

EDI ECommerce and Multiple Domains

◆ See *User Guide Volume 7: Release Management* for information on EDI ECommerce.

This chapter includes information on setting up and using EDI ECommerce in a multiple-domain environment.

Overview **174**

Multiple-Domain Processing **174**

Multiple-Domain Setup **176**

Overview

EDI ECommerce has been enhanced so that you can use a single instance of ECommerce to import and export documents between multiple MFG/PRO domains and the EC subsystem.

This chapter describes how the system processes EDI transactions and how you set up multiple domain features.

Multiple-Domain Processing

The primary factor the system uses in determining how to process EDI transactions in a multiple-domain environment is the ECommerce processing domain—the domain in which repository records and MFG/PRO business documents are stored. This domain is one of the following:

- By default, the log-in domain of the EDI ECommerce user—either at initial log-in or modified using Change Current Domain (36.10.1)
- The processing domain specified after log-in using Change Current ECommerce Domain (35.11.11)
- The domain associated with the user's log-in domain in Domain Cross-Reference Maintenance (35.11.1)

In some cases, all EDI ECommerce processing and document creation happens within a single domain. For example, the user who imports a purchase order is logged in to the same domain where the resulting sales order will be created. System-generated repository records are in the user's domain, so that error-reporting and repository maintenance functions have direct access to the records that the transformation and gateway processes use to create the sales order.

In a different scenario, the user might not create records in the log-in domain, based on one of the following factors:

- ◆ See “Specifying Domain Cross-References” on page 177.

 - A record created in Domain Cross-Ref Maintenance associates the user's log-in domain and a second domain used for ECommerce processing.

- A domain identifier in the transformation definition sets the value of the DOMAIN token during transformation. In this case, a token variable set to this value causes the document to be created in the EDI ECommerce processing domain. However, the MFG/PRO transaction data is created in a different domain.

◆ See “Changing the Target Domain During Transformation” on page 178.

In either of these cases, the system can load repository data and create the MFG/PRO business document—the sales order, for example—in a different domain than where the user is logged in.

Note If any user transformation functions were defined prior to the release of multiple-domain functionality, you must update them to reference an additional Progress include file and a domain-associated variable used during transformation.

◆ See “Updating Existing User-Defined Functions” on page 179.

During export, the system similarly uses either the user’s session log-in domain or a cross-reference record to determine the ECommerce processing domain that provides domain-specific data—such as trading partner information—for outbound documents. It uses the DOMAIN variable for reference to determine the correct source domain for exported data, including any turnaround data.

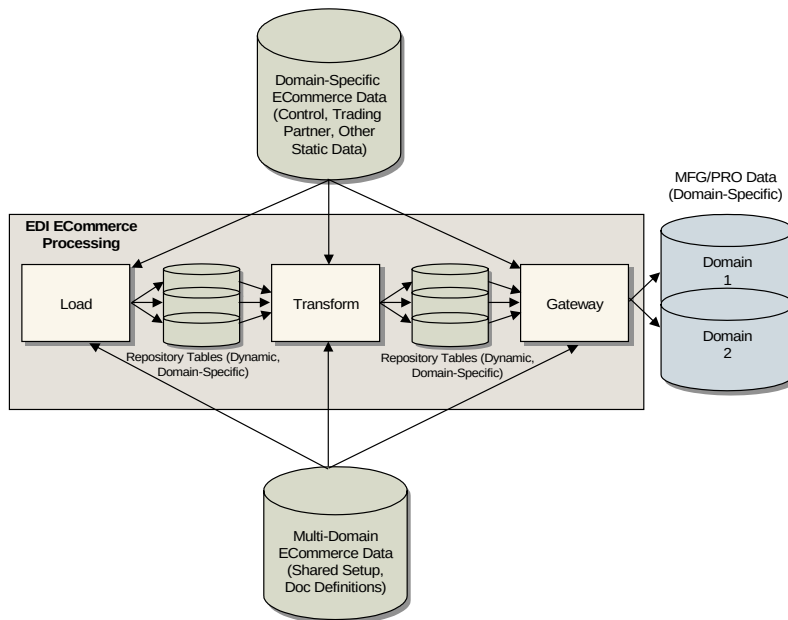
Turnaround data is stored based on the ECommerce processing domain used when the source document is imported. When you update turnaround data using Turnaround Data Maintenance (35.9.17), use the Target Domain field to specify the domain associated with the turnaround data you want to maintain. You also can specify the target domain when you archive and delete turnaround data using Turnaround Data Archive/Delete (35.17.16).

Note When you use a single-domain MFG/PRO database, the domain is essentially transparent to the EDI ECommerce setup and processing functions. No special setup or implementation steps are needed, with the exception of updating existing user-defined functions that access the database to let them handle system-required domain values.

◆ See “Updating Existing User-Defined Functions” on page 179.

Figure 5.1 is an overview of how EDI ECommerce processes documents in a multiple-domain environment.

Fig. 5.1
EDI ECommerce
Multiple-Domain
Processing Flow



Multiple-Domain Setup

The majority of data-intensive records—including the exchange file, MFG/PRO document, implementation, and transformation definitions—are shared by all the domains in a database. However, to use the product in a multiple-domain environment, several kinds of data must be set up in each domain. These types of data are records that typically vary between domains, such as trading partner records and control settings.

Note Each domain has its own ECommerce Control (35.13.24) record. This lets you set up different inbound directories so that the location where the system looks for imported files can vary by log-in domain.

To enter domain-specific setup data, either log in to the target domain at sign-on or switch to the appropriate domain using Change Current Domain (36.10.13) or Change Current ECommerce Domain (35.11.11). The system automatically assigns the records you create to the appropriate ECommerce processing domain.

Table 5.1 lists the programs used to set up required domain-specific records.

Program	Menu	Comments
Turnaround Data Maintenance	35.9.17	
EC Subsystem/Exchange Maint	35.13.3	
EC Subsystem/MFG Maint	35.13.5	
Trading Partner Maintenance	35.13.7	
Trading Partner Parameter Maint	35.13.10	
Data Cross-Reference Maintenance	35.13.16	Optional functionality
Data Validation Maintenance	35.13.21	Optional functionality
ECommerce Control	35.13.24	

Table 5.1
Domain-Specific
Setup Programs

When you are loading new data from trading partner library files rather than entering it manually using one of the listed programs, the system automatically separates domain-specific information and loads it into the EDI ECommerce domain you specify during the load process.

◆ See “Loading Trading Partner Library Records” on page 179.

Specifying Domain Cross-References

By default, EDI ECommerce processing is based on the domain of the logged-in user session. The system uses domain-specific setup records, looks for MFG/PRO data associated with that domain, and generates repository records using that domain as a key field. However, in some EDI environments, not all of those elements are in the log-in domain. For example, a centralized EDI processing area that supports several domains can load data for each domain individually, but can maintain the EDI data within a central domain.

Use Domain Cross-Reference Maintenance (35.11.1) to set up a cross-reference record between the user’s MFG/PRO log-in domain and a domain used in EDI ECommerce processing.

Tip
The values of both fields must be defined in Domain Maintenance (36.10.1).

The system uses a cross-reference record under either of the following circumstances:

- The user’s log-in domain is the same as the specified value.
- The user changes to this domain using Change Current Domain (36.10.13).

When no cross-reference records are set up, the system uses the log-in domain of the user as the ECommerce domain. To switch to a different processing domain during a session, use Change Current ECommerce Domain (35.11.11).

Note No cross-reference records are needed in a single-domain environment.

Fig. 5.2
Domain Cross
Reference
Maintenance
(35.11.1)

Changing the Target Domain During Transformation

By default, during document import the system creates MFG/PRO repository documents and the resulting business documents—such as sales orders—in the ECommerce processing domain. It also is possible to have the system map the document to a different domain by assigning a target domain during transformation.

Use Transformation Definition Maintenance (35.15.17) to specify an event action that determines the domain associated with the document. For example, the event action shown in Figure 5.3 assigns the domain variable a value of 1. The import gateway associated with the transformation creates the resulting document in domain 1.

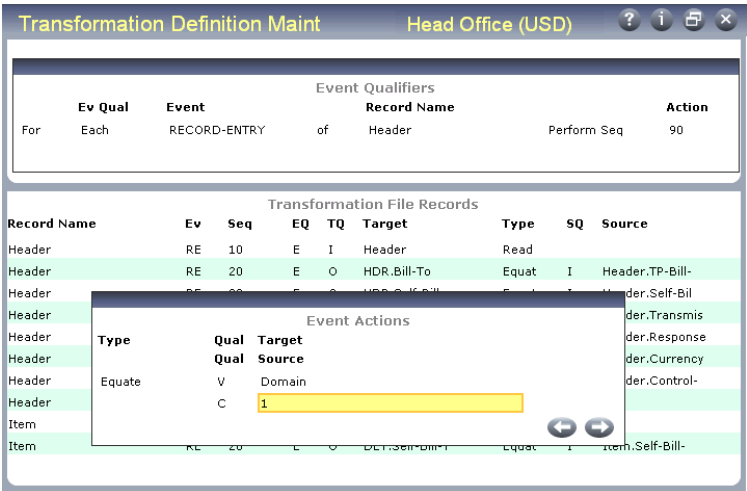


Fig. 5.3
Transformation
Definition
Maintenance
(35.15.17), Event
Action Example

Loading Trading Partner Library Records

Although most elements added by Trading Partner Library Load (35.17.7) are shared by all domains, several kinds of data are domain specific.

Use the Target Domain field to specify which domain the domain-specific parts of the new setup data will be associated with. The field defaults from the user’s log-in domain. You can change it to any valid domain defined in Domain Maintenance (36.10.1).

Updating Existing User-Defined Functions

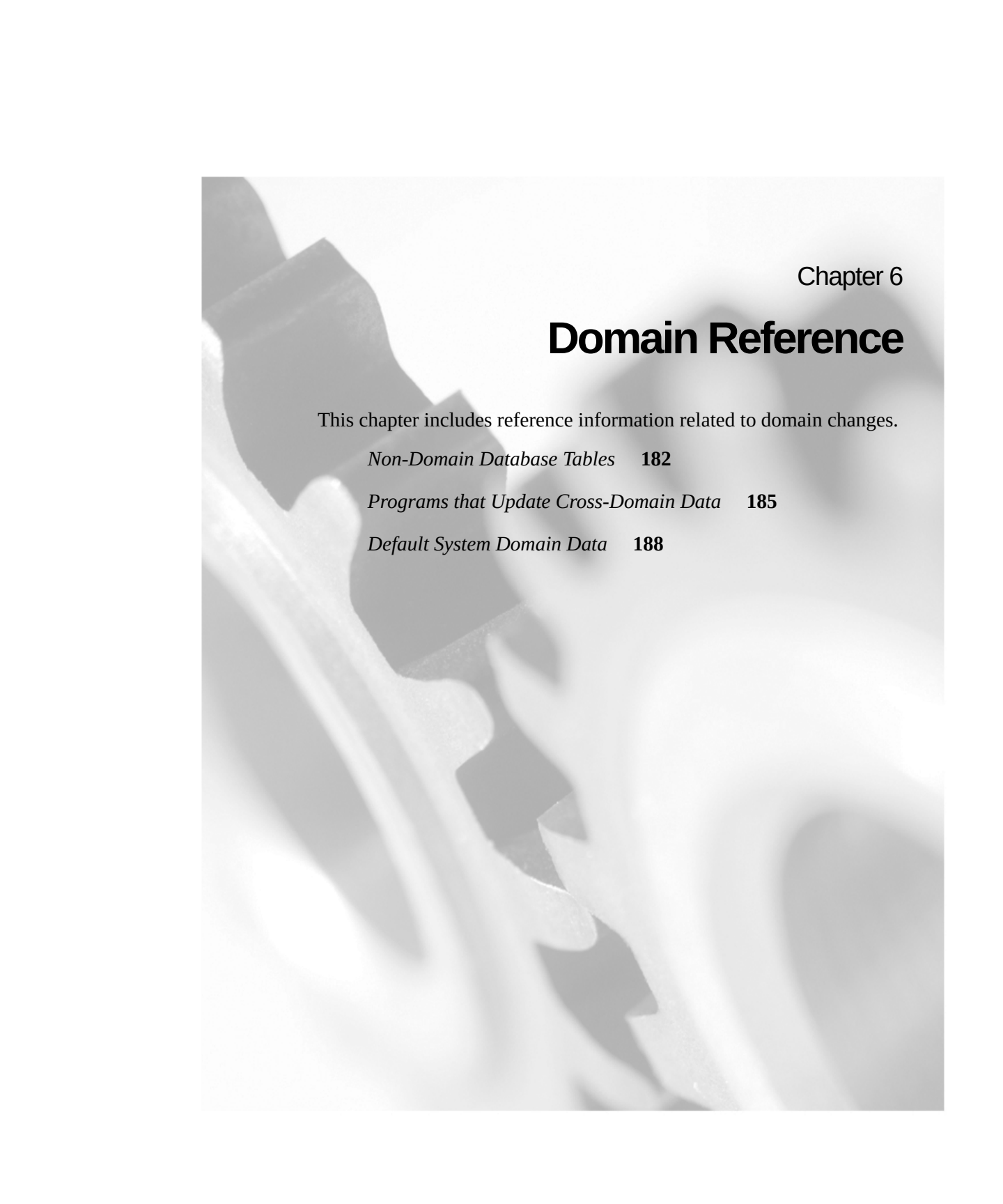
EDI ECommerce has been modified to add a new shared variable to user-defined transformation functions when you generate them using ECommerce Function Maintenance (35.15.21). This new variable, `trgt_domain`, lets new functions identify the correct domain associated with the data that the function will access or process. For example, it is used to set the target domain to the value of the `DOMAIN` token.

You must update the code for any existing functions that access the database to let them continue to support transformation with no risk of degrading processing performance. Additionally, the functions should have a reference to the Progress include file `mgdomain.i`.

To update user-defined functions, use a text editor to add the following code to the beginning of each Progress function program:

```
{mgdomain.i}  
define shared variable trgt_domain like global_domain no-undo.
```

User-defined functions are stored in the directory specified in the Function Directory field in ECommerce Control (35.13.24).

The background of the page is a grayscale image of several interlocking gears. The gears are of different sizes and are positioned in a way that they appear to be meshing together. The lighting creates highlights and shadows on the teeth of the gears, giving them a three-dimensional appearance. The overall tone is technical and mechanical.

Chapter 6

Domain Reference

This chapter includes reference information related to domain changes.

Non-Domain Database Tables **182**

Programs that Update Cross-Domain Data **185**

Default System Domain Data **188**

Non-Domain Database Tables

Table 6.1 lists the tables in the MFG/PRO database that do not include domain information. These tables contain data that is shared among all domains in a database.

Table 6.1
Non-Domained
Tables

Table	Description
abd_det	Asset Book Detail
accd_det	Asset Cost Change Detail
ast_mstr	Asset Master
atak_det	Audit Trail Activated Key Detail
atap_mstr	Audit Trail Activated Profile Master
atc_ctrl	Audit Trail Control
atdc_mstr	Audit Trail Database Connection Master
aterr_mstr	Audit Trail Error Master
atgt_ref	Audit Trail Group – Table Cross-Reference
atg_mstr	Audit Trail Group Master
attmp_mstr	Audit Trail Temporary Master
att_mstr	Audit Trail Table Master
atwk_det	Audit Trail Workbench Key Detail
atwp_mstr	Audit Trail Workbench Profile Master
bkfm_mstr	Bank Account Format Master
ccd1_det	Cost Center/Account Validation Detail
ccd2_det	Cost Center/Sub-Account Validation Detail
cls_mstr	Class Master
cst_mstr	Fixed Asset Custodian Master
ctry_mstr	Country Master
cu_mstr	Currency Master
dbk_mstr	Depreciation Book Master
dbm_mstr	Database Revision Control Master
dc_mstr	Database Connection Master
dmw_wkfl	Draft Management Work Table
dom_mstr	Domain Master

Table 6.1 — *Non-Domained Tables* — (Page 1 of 4)

Table	Description
dpc_mstr	Depreciation Convention Master
dpr_mstr	Depreciation Method Master
dprd_det	Depreciation Detail
dprt_det	Depreciation Method Detail
em_mstr	E-mail Master
esapfc_det	E-Signature Activated Profile Filter Criteria
esapfil_det	E-Signature Activated Profile Filter
esapfs_det	E-Signature Activated Profile Filter Set
esapf_det	E-Signature Activated Profile Field
esamp_ref	E-Signature Activated Profile Menu Program Cross-Reference
esaps_det	E-Signature Activated Profile Structure
esap_mstr	E-Signature Activated Profile
escat_mstr	E-Signature Category Master
escd_det	E-Signature Category Detail
escf_ref	E-Signature Category Filter Cross-Reference
escx_det	E-Signature Category XML Detail
esfil_mstr	E-Signature Filter
esgc_ref	E-Signature Group Category Cross-Reference
esig_mstr	E-Signature Master
esrec_det	E-Signature Record List
eswpfc_det	E-Signature Workbench Profile Filter Criteria
eswpfil_det	E-Signature Workbench Profile Filter
eswpfs_det	E-Signature Workbench Profile Filter Set
eswpf_det	E-Signature Workbench Profile Field
eswmp_ref	E-Signature Workbench Profile Menu Program Cross-Reference
eswps_det	E-Signature Workbench Profile Structure
eswp_mstr	E-Signature Workbench Profile
exru_usage	Exchange Rate Usage
fal_mstr	Fixed Asset Location Code Master
fas_ctrl	Fixed Asset System Control
fldf_mstr	Field Default Master
flh_mstr	Field Help Program Master

Table 6.1 — *Non-Domained Tables* — (Page 2 of 4)

Table	Description
hlp_mstr	Help Master
lblc_ctrl	Label Control
lng_mstr	Language Master
lngd_det	Language Detail
max_mstr	Maximums Master
maxt_det	Maximum Table Detail
mfrel_mstr	Master Table Relationships
mnd_det	Menu Detail
mnt_det	Menu Title Detail
msg_mstr	Message Master
pr_mstr	Printer Master
prd_det	Printer Detail
qaddb_ctrl	Database Control for QADDB
sbd_det	Sub-Account/Account Validation Detail
syp_mstr	Sync Profile Master
sypd_det	Sync Profile Detail
sypj_det	Sync Profile Join Detail
syys_det	Sync Profile Subscription Detail
sytf_mstr	Sync Table-Field Master
tax_mstr	Tax Master
taxd_det	Tax Detail
typ_mstr	Fixed Asset Type Master
tzo_mstr	Service/Support Time Zone Master
tzod_det	Service/Support Time Zone Detail
ufd_det	User Function Key Detail
upd_det	Printer/User Detail
url_mstr	URL Master Table
usg_det	Application Usage Detail
uslh_hist	User Logon History
uspw_hist	User Password History
usr_mstr	User Master
usrc_ctrl	User Control

Table 6.1 — *Non-Domained Tables* — (Page 3 of 4)

Table	Description
usrg_mstr	User Group Master
usrl_det	User Licensed Application Detail
vt_mstr	Value Added Tax Master
vtc_ctrl	Value Added Tax Control

Table 6.1 — *Non-Domained Tables* — (Page 4 of 4)

Programs that Update Cross-Domain Data

Some functions in MFG/PRO update data that is shared across domains. Table 6.1 lists functions that update this kind of data. The corresponding reports and browses also display shared data, but are not included in this table. For example, if Country Code Maintenance updates shared data, you can assume that Country Code Browse and Report display shared data.

Menu No.	Program Description	Name
2.14.1	Country Code Maintenance	adctrymt.p
3.21.19	Transaction Numbering Report	ictrnrp.p
17.22	Operations Numbering Report	reopnrp.p
18.16	Operations Numbering Report	reopnrp.p
26.6	Exchange Rate Relationship Maintenance	mcdexrmt.p
26.7	Derived Exchange Rate Calculation	mcdexrcc.p
35.13.13	Transmission Group Maintenance	edtgmt.p
35.13.19	HTTP Adapter Maintenance	edhttpmt.p
35.15.6	Exchange Definition Maintenance	edxfmt.p
35.15.10	MFG/PRO Definition Maintenance	edmfmt.p
35.15.13	Implementation Definition Maint	edmimt.p
35.15.17	Transformation Definition Maint	edtrmt.p
35.15.21	ECommerce Function Maintenance	edtrfmt.p
36.2.1	Drill Down/Lookup Maintenance	mgdlfhmt.p
36.2.4	User Tool Maintenance	mgtoolmt.p
36.2.6	Menu Substitution Maintenance	mgmsmt.p

Table 6.2
Programs Updating
System-Wide Data

Table 6.2 — *Programs Updating System-Wide Data* — (Page 1 of 4)

Menu No.	Program Description	Name
36.2.13	Browse Maintenance	mgbwmt.p
36.2.18	View Maintenance	mgvwmt.p
36.3.1	User Maintenance	mgurmt.p
36.3.3	User Password Maintenance	mgurmt.p
36.3.4	User Group Maintenance	mgurgpmt.p
36.3.10	Menu Security Maintenance	mgpwmt.p
36.3.11	Menu Security Change	mgpwcg.p
36.3.21.1	Program Information Maintenance	mgpgmimt.p
36.3.21.3	Rule Maintenance	mgrulemt.p
36.3.21.5	Constant Maintenance	mgcnstmt.p
36.3.21.7	Profile Maintenance	mgprofmt.p
36.3.21.9	Profile Program Maintenance	mgprpgmt.p
36.3.21.11	Profile Program Rule Maintenance	mgpprlmt.p
36.3.21.14	Group Maintenance	mggrpmt.p
36.3.21.16	Group Constants Values Maint	mggrcnmt.p
36.3.21.18	User Group Security Maintenance	mgursmt.p
36.3.21.20	User Constants Value Maintenance	mguscnmt.p
36.3.21.24	Desktop Security Control	mgsecpm.p
36.3.21.23.21	Browse UI Records Maintenance	mgusrbmt.p
36.3.24	Security Control	mgurpmmt.p
36.4.1	Language Code Maintenance	mgllmt.p
36.4.3	Language Detail Maintenance	mglngumt.p
36.4.4	Menu System Maintenance	mgmemt.p
36.4.7	Message Maintenance	mgmsgmt.p
36.4.11	User Function Maintenance	mgufmt.p
36.4.13	Field Help Maintenance	mgflhusr.p
36.4.17.1	Label Master Maintenance	gplblmt.p
36.4.17.5	Label Detail Maintenance	gplbldmt.p
36.4.17.24	Label Control	gplblpm.p
36.4.18	Field Help Dump	mgfldmp.p
36.4.19	Field Help Load	mgflld.p
36.4.20	E-Mail Definition Maintenance	mgemmt.p

Table 6.2 — Programs Updating System-Wide Data — (Page 2 of 4)

Menu No.	Program Description	Name
36.6.1	Database Connection Maintenance	mgdcmt.p
36.6.13	Database Connect	mgdccn.p
36.6.15	Database Disconnect	mgdcdc.p
36.8.16	Export/Import Document Query	qqbr.p
36.8.17	Export/Import Document Report	qqierp.p
36.8.18	Dump Export/Import Docs to File	qqwrt.p
36.8.22.1	Synchronization Profile Maintenance	qqsypmt.p
36.8.22.3	Sync Table–Field Maintenance	qqsytfmt.p
36.8.22.8	Synchronization Mass Export	qqsymsex.p
36.10.1	Domain Maintenance	mgdommt.p
36.10.13	Change Current Domain	mgdomchg.p
36.12.13.1	Audit Trail Group Maintenance	attgmt.p
36.12.13.4	Audit Workbench Refresh	atwpref.p
36.12.13.5	Audit Workbench Profile Maintenance	atwpmt.p
36.12.13.8	Audit Profile Activation	atwpact.p
36.12.13.11	Audit DB Maintenance	atdbmt.p
36.12.13.23	Audit Trail Creation Process	atttpui.p
36.12.13.24	User Accountability Control	atpm.p
36.12.14.1	E-Signature Group Maintenance	escgmt.p
36.12.14.4	E-Signature Workbench Refresh	eswpref.p
36.12.14.5	E-Sig Workbench Profile Maint	eswpmt.p
36.12.14.8	E-Signature Profile Activation	eswpact.p
36.12.14.21	E-Sig Failure Archive/Delete	esesigup.p
36.12.14.22	E-Signature Archive/Delete	esesup.p
36.12.14.23	E-Signature Restore	esesld.p
36.13.1	Printer Type Maintenance	mgmgmt04.p
36.13.2	Printer Setup Maintenance	mgmgmt05.p
36.13.4	Printer Default Maintenance	mgupmt.p
36.13.13	Print Queue Maintenance	mgmgmt07.p
36.14.3	Batch Request Detail Maintenance	mgbcdmt.p
36.14.13	Batch Request Processor	mgbatch.p
36.16.10.1	License Registration	lvreg.p

Table 6.2 — Programs Updating System-Wide Data — (Page 3 of 4)

Menu No.	Program Description	Name
36.16.13	Sequence Maintenance	msgsqmt01.p
36.16.17	Database Sequence Initialization	utsequp.p
36.16.22.1	Multiple Time Zones Maintenance	fstzomt.p
36.16.22.13	Multiple Time Zone Load Utility	uttzld.p
36.19.1	AppServer Service Maintenance	mgasmt.p
36.20.10.1	User Option Maintenance	mgusromt.p
36.20.10.3	User Option Telnet Maintenance	mgusrmt.p
36.20.10.8	Menu URL Maintenance	mgurlmt.p
36.20.10.11	Browse URL Maintenance	mgburlmt.p
36.20.10.15	Session Master Maintenance	mgssmt.p
36.22.1	Exit to Operating System	mgoscall.p
36.22.3	Program Execute	mgmgmt24.p
36.22.4	Program/Text File Display	mgfdsply.p
36.22.13	Disk Space Inquiry	mgdfds.p
36.24	Database Control	mgdbpm.p

Table 6.2 — *Programs Updating System-Wide Data* — (Page 4 of 4)

Default System Domain Data

Table 6.3 lists database tables containing data that is copied when a new domain is created.

Table 6.3
Tables Copied for
New Domain

Table	Description
acdf_mstr	Account Default Master
ad_mstr	Address Master
apc_ctrl	Accounts Payable Control
arc_ctrl	Accounts Receivable Control
bic_ctrl	Service/Support Contract Billing Control
bk_mstr	Bank Master
bl_ctrl	Master Bill of Lading Control
cac_ctrl	Service/Support Call Master Control
caq_mstr	Service/Support Call Queue Master

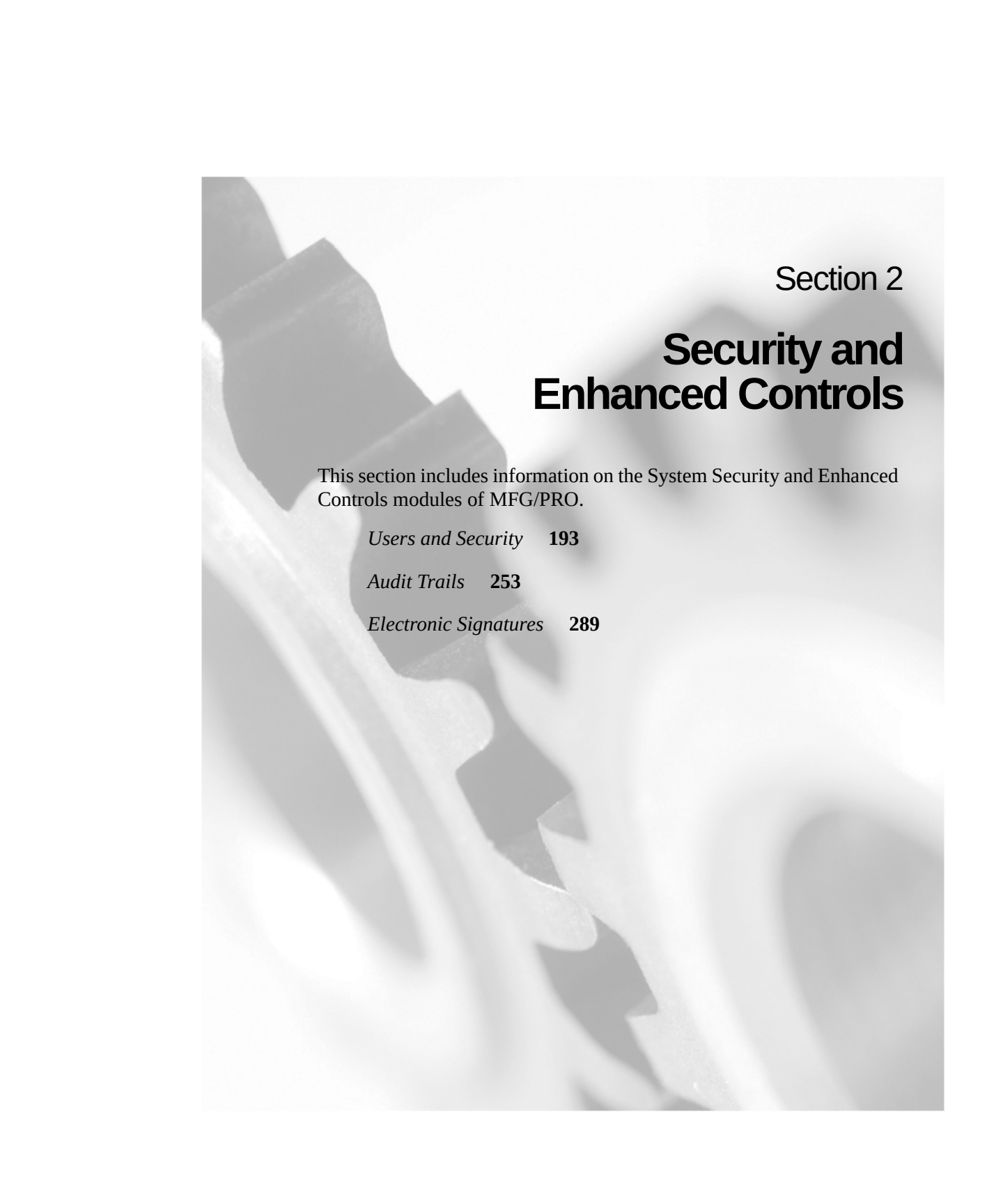
Table 6.3 — *Tables Copied for New Domain* — (Page 1 of 3)

Table	Description
cas_mstr	Service/Support Call Status Master
cc_mstr	Cost Center Master
cd_det	Master Comments
cfc_ctrl	Cash Flow Control
clc_ctrl	Compliance Control
cmc_ctrl	Customer Control
co_ctrl	General Ledger (Company) Control
code_mstr	Generalized Code Master
cr_mstr	Code Range Master
cs_mstr	Cost Set Master
drp_ctrl	Distribution Requirements Planning Control
egc_ctrl	Service/Support Engineer Schedule Control
emc_ctrl	Employee Control
es_mstr	Service/Support Escalation and Repair Master
esc_ctrl	Service/Support Escalation Control
esh_mstr	Service/Support Engineer Schedule Master
ess_mstr	Service/Support Engineer Status Master
et_ctrl	EMU Control
fac_ctrl	Final Assembly Control
famt_mstr	Fixed Asset Method Master
gl_ctrl	System/Account Control
icc_ctrl	Inventory Control
iec_ctrl	Import/Export Control
ls_mstr	Address List Detail
mfc_ctrl	Control Work Table
mrpc_ctrl	Material Requirements Planning Control
opc_ctrl	Shop Floor Operation History Control
pcc_ctrl	Product Change Control
pgc_ctrl	Service/Support Paging Control
pic_ctrl	Pricing Control
pj_mstr	Project Master
pl_mstr	Product Line Master

Table 6.3 — *Tables Copied for New Domain* — (Page 2 of 3)

Table	Description
poc_ctrl	Purchase Order Control
qcc_ctrl	Quality Order Control
qoc_ctrl	Sales Quotation Control
rnc_ctrl	Return Material Authorization Control
rnd_mstr	Rounding Method Master
rpc_ctrl	Repetitive Control
rsn_ref	Reason Code Master
sac_ctrl	Service Contract Control
sb_mstr	Sub-Account Master
sbc_mstr	Service/Support Billing Cycle Master
sc_mstr	Cost Simulation Master
shop_cal	Shop Calendar
soc_ctrl	Sales Order Control
spc_ctrl	Salesperson Control
src_ctrl	Service Request Control
sroc_ctrl	Service/Repair Order Control
sv_mstr	Service Agreement Terms and Conditions Master
svc_ctrl	Service/Support Management Control
trl_mstr	Trailer Master
tx2_mstr	Tax Master
txc_ctrl	Tax Control
vdc_ctrl	Supplier Control
woc_ctrl	Work Order Control

Table 6.3 — *Tables Copied for New Domain* — (Page 3 of 3)

The background of the page features a grayscale image of several interlocking gears. The gears are of different sizes and are positioned in a way that creates a sense of depth and mechanical complexity. The lighting is soft, highlighting the teeth of the gears and creating subtle shadows.

Section 2

Security and Enhanced Controls

This section includes information on the System Security and Enhanced Controls modules of MFG/PRO.

Users and Security **193**

Audit Trails **253**

Electronic Signatures **289**

Users and Security

This chapter describes how to set up users and manage different kinds of security.

Note For MFG/PRO eB2.1, this chapter replaces Chapter 3 in *MFG/PRO eB2 User Guide Volume 9: Manager Functions*.

Security in MFG/PRO **194**

Security Overview **195**

Setting Up Security Control **213**

Defining Users **223**

Controlling Access with User Groups **234**

Using Security Functions **238**

Monitoring System Security **250**

Security in MFG/PRO

MFG/PRO security and related technical controls must be viewed within the context of an organization's overall security framework. While it is beyond the scope of this user guide to discuss the details of information security, the fundamental components involve measures to assure the preservation of:

- Confidentiality—ensuring that information is accessible only to those authorized to have access
- Integrity—safeguarding the accuracy and completeness of information and processing methods
- Availability—ensuring that authorized users have access to information and associated assets when required

► See *User Guide Volume 9: Manager Functions*.

For MFG/PRO, availability includes items such as policies and procedures for data, equipment, and infrastructure backup and recovery. Features that can support these items are discussed in other sections of the user guide.

Security properly starts with a comprehensive policy statement that:

- Clearly demonstrates management's support and commitment to security
- Defines the principle security components important to the organization
- Describes the general approach for meeting security objectives

After the policy statement is prepared, procedures, guidelines, and other supporting administrative controls are typically defined to support the policy. Finally, technical controls such as those described in this chapter are designed and implemented to support the administrative controls.

► See "Security Planning Checklists" on page 210.

This chapter includes several checklists to use as starting points in planning and implementing a comprehensive security plan to meet the specific security requirements of your environment.

The specific level of security control an organization should implement is a function of the underlying information security requirements. Those requirements originate:

- Externally, including regulatory, legal, and legislative requirements

- Internally, based on the value of information assets, associated risks to those assets, and available controls that can eliminate or mitigate exposures to an acceptable level

Much of the security control in MFG/PRO is designed to support external requirements. Numerous controls have been introduced to support MFG/PRO customers who are concerned with meeting the security requirements of legislation and regulations such as the Sarbanes-Oxley Act and Food and Drug Administration 21 CFR Part 11.

Security Overview

MFG/PRO provides options for security on several levels, based on information defined in user master records.

Two types of security are enforced at log-in:

- Log-in security determines whether a user can log in to an MFG/PRO session. This level of security is always active and requires that users specify a valid user ID and password before they can log in.

◆ See “Basic Log-In Security” on page 198.

Optionally, system administrators can choose to bypass MFG/PRO log-in security and automatically log in valid users based on operating system-level access.

◆ See “OS-Based Log-in Security” on page 200.

Note You also should consider additional access security options at the operating-system and Progress levels.

- Domain security limits individual user access to specific domains identified in User Maintenance. Users are limited to authorized domains at log-in. Additionally, the system controls domain access when the user runs Change Current Domain (36.10.13), as well as certain programs that can display or update records from multiple domains.

◆ See “Operating System and Progress Security” on page 201.

Other security methods are based on what action the user is attempting within the system. Individual programs let you control access based on individual user IDs and/or user groups:

◆ See “Using Security Functions” on page 238.

- Menu security (36.3.10) limits access to menus and menu functions.
- Field security (36.3.19) limits who can update specific fields.

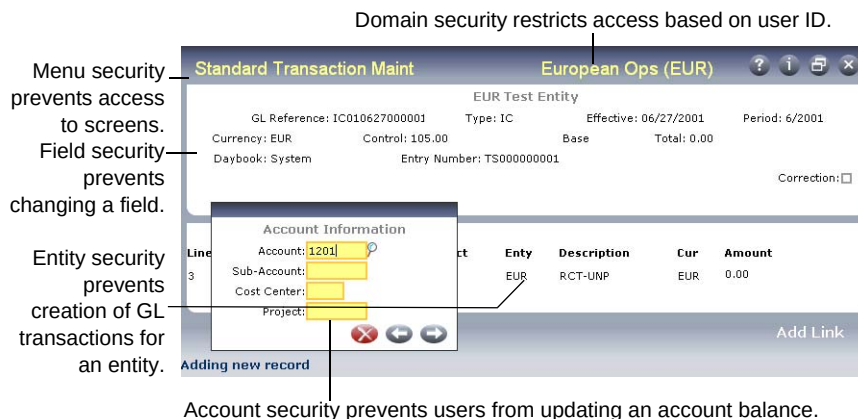
- Entity security (36.3.13) limits who can create GL transactions for a particular entity.
- Site security (36.3.15) limits who can create inventory transactions at secured sites.
- General ledger (GL) account security (36.3.16) restricts access to GL accounts.
- Inventory movement security (36.3.17) lets you grant or deny group members access to shippers and other transactions using specific movement codes at a site.

► See *External Interface Guide: Sales and Use Tax* for information on SUTI.

Note If you use the Sales and Use Tax Interface (SUTI) to communicate tax data between MFG/PRO and Vertex’s Quantum for Sales and Use Tax product, set up similar access controls in Tax Interface Control (36.5.3.24).

Figure 7.1 illustrates how several different kinds of security can operate at the same time with the same user.

Fig. 7.1
Types of Security



► See “Using Security Functions” on page 238.

► See “Controlling Access with User Groups” on page 234.

Security functions use user IDs and groups for system elements controlled by menu, site, entity, and so on. The security maintenance function creates a record that pairs a field or function and user IDs or user groups.

- For menu security, site security, GL account security, and inventory movement code security, specify any combination of user IDs or user group names.
- For entity and field security, specify user IDs.

- For domain security, grant each individual user access in User Maintenance.

When a user tries to do something that is controlled by security, the system compares the security records with the ID and groups associated with the current user. If there is a match, the system grants or limits the user's actions accordingly.

Another layer of access security is specific to QAD Desktop. Desktop security (36.3.21) lets you restrict who can log in to a database using the Desktop interface. It also provides a detailed and focused way of controlling access to data when browses and reports are generated from the Desktop.

▶ See *User Guide: QAD Desktop* for details.

Important The various MFG/PRO security controls are primarily effective within an MFG/PRO session. The MFG/PRO database should be protected from any unauthorized access, not just access from within an MFG/PRO session. Additional controls should be considered to prevent compromise of MFG/PRO data using other means.

▶ See “Operating System and Progress Security” on page 201.

Password Management

MFG/PRO offers a flexible approach to assigning and managing passwords, based on the specific requirements of each environment.

Settings in Security Control (36.3.24) determine how passwords are generated, structured, and controlled. Your strategy can be as complex or as simple as required to meet requirements. You can specify:

▶ See “Create a Password Strategy” on page 219.

- The minimum length of the password, including minimum numbers of numeric and non-numeric characters
- The number of days passwords are valid and whether the system begins warning users of the expiration date a given number of days in advance
- The number of days or password change cycles that must pass before a user can reuse the same password
- The manual or automatic method used to generate temporary passwords

Example In a high-security environment, you might specify an eight-character password that must contain at least three numbers. Users must change passwords every 60 days, and are warned each time they log in within 10 days of expiration. To prevent even the system administrator from knowing individual passwords, the system is set up to automatically generate new temporary passwords and e-mail them directly to each user. Users must then create their own passwords at the first log-in using the temporary password—subject to the parameters defined in Security Control.

◆ See “Updating Passwords” on page 230.

In case of forgotten or compromised passwords, User Maintenance (36.3.1) lets system administrators force an individual user to change the password at next log-in. User Password Force Change Utility (36.3.23.12) makes all users or members of specified groups change their passwords.

Basic Log-In Security

◆ See “Setting Up Security Control” on page 213.

Typically, a user must enter both a user ID and a password to log in to MFG/PRO. If the user enters an invalid combination, the system may prompt additional times—based on the value of Maximum Access Failures in Security Control. After the specified number of failures, the user is returned to the operating system, the user account is deactivated, and members of the system administration group are notified by e-mail. The sending address of the e-mail includes the operating system ID of the user who attempted to access MFG/PRO. Figure 7.2 illustrates how this process occurs during log-in.

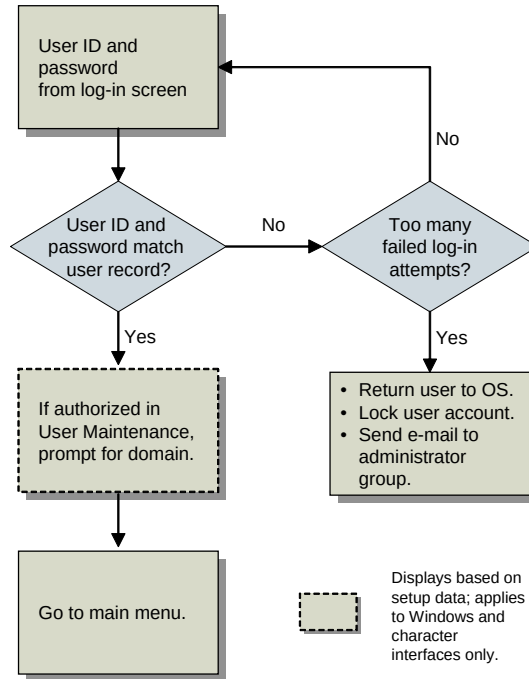
◆ See “OS-Based Log-in Security” on page 200.

Note To completely or partially bypass MFG/PRO log-in security, you can configure the system to allow users to access the system based on operating system user ID.

Depending on the setting specified in Security Control, the system maintains historical records of successful and failed log-in attempts. Use Logon Attempt Report (36.3.23.1) to view log-in history.

◆ See “Setting a Default Time Zone” on page 67.

Note In order for the time zone to be properly recorded during log-in and password change, the server time zone must be specified in Database Control (36.24).

Fig. 7.2
Log-In Validation

This type of log-in security lets you:

- Unless you choose to control access from the operating system level, effectively separate MFG/PRO security from the operating system security. The user ID in MFG/PRO does not have to be the same as the user ID referenced by UNIX or Windows.
- Provide an extra level of security from unauthorized users. An individual can gain access to an operating system user ID by breaking into the system or stealing a password. Requiring a different user ID and password combination to access MFG/PRO presents an additional barrier to an unauthorized user.
- Track unsuccessful log-in attempts to identify possible unauthorized efforts to access the system.

♦ See “OS-Based Log-in Security” on page 200.

To provide maximum security, the system does not save log-in related data from session to session. MFG/PRO user interfaces typically require users to enter both a valid user ID and a password at each log-in unless you choose to control access directly from the operating system level.

OS-Based Log-in Security

► See “Setting Up Security Control” on page 213.

System administrators can control user access to MFG/PRO character and Windows environments directly from the operating-system level using the Enforce OS User ID field in Security Control (36.3.24).

If they do not use passwords in MFG/PRO, this feature essentially allows customers using those interfaces to bypass MFG/PRO log-in security completely and rely on operating-system security.

Important Regardless of this setting, QAD Desktop users must enter a valid user ID and password to access the system.

When Enforce OS User ID is Yes, the default user ID displayed in the log-in screen is the same ID used by the operating system, and the user cannot change it.

Note This must still be a valid MFG/PRO user ID defined in User Maintenance (36.3.1).

Subsequent processing depends on whether a password is specified in User Maintenance or User Password Maintenance (36.3.3):

- If no password is specified in the MFG/PRO user record, log-in proceeds automatically, subject to proper licensing.
- If the user record includes a password, the system displays a password prompt.

Important If you enable this feature and reset MFG/PRO user passwords to blank, you should use caution if Enforce OS User ID is ever changed to No. If you do so without reentering passwords in user records, anyone can gain access to MFG/PRO by entering just a user ID. When you change the field from Yes to No, the system displays a message to warn you of a potential security compromise. In addition, in Windows environments it is not recommended that you reset MFG/PRO user passwords to blank. It is relatively easy to create a new user on an existing Windows machine with an ID that matches one in MFG/PRO.

Domain Security

Access to domains is controlled at two points:

- During system log-in
- During the MFG/PRO session

By default, the system logs users in to the domain defined as the default in User Maintenance. Depending on your user interface, you may be able to switch to a different domain during log-in:

◆ See “Specifying Domains” on page 231.

- Windows and character interfaces. When your User Maintenance record gives you access to multiple domains, the system displays a Domain field after you enter a correct user ID/password combination. You can change it to any active domain associated with your user ID.
- QAD Desktop. The log-in screen does not currently include a domain field. The system logs you in to your default domain.

Note Starting with version 2.7 of QAD Desktop, you can change your domain at any time using a drop-down provided on the QAD Desktop main page.

When your User Maintenance record specifies more than one domain, you can switch domains after log-in using Change Current Domain (36.10.13). However, the system never lets you access a domain that is not authorized in your user record.

◆ See “Changing the Current Domain” on page 63.

Operating System and Progress Security

MFG/PRO security controls applied using programs on the Security Menu (36.3) apply primarily to accessing the application itself, as well as accessing functions within the application. In addition to MFG/PRO controls, you should consider additional security at the operating system and Progress levels.

At the operating system level, all MFG/PRO-related files should be reviewed to determine the appropriate permission and ownership settings. Relevant files would include at a minimum:

- Database files (*.db)
- Log files (*.lg)
- Source code files (*.p)

- Compiled source code (*.r)
- Database backup files
- Files used to execute system administration tools such as MFG/UTIL

For example, on UNIX platforms, a system administrator should be the owner for most—if not all—of these files. To restrict access to these files, operating system commands such as the following for UNIX can be used to limit both Read and Write access to the file owner.

```
chmod 600 <database file name>
```

The standard Progress documentation set provides information about security controls, including the following documents:

- *Database Administration Guide*
- *Client Deployment Guide*
- *Progress Programming Handbook*

The following sections discuss information-security exposures and mitigating controls in these areas:

- Accessing the Progress Editor from MFG/PRO
- Capabilities to directly read, modify, and delete database records
- Compiling custom code on unprotected databases
- Accessing an MFG/PRO database directly from Progress

Progress Editor Access

One area of potential security exposure is related to the Progress Editor. By default, legitimate MFG/PRO users can access the Progress Editor by exiting from the MFG/PRO menu and specifying the appropriate code at the exit prompt. Once a user has accessed the Progress Editor, MFG/PRO data can be significantly exposed.

► See “Assign Access by Menu” on page 240.

You can use Menu Security Maintenance (36.3.10) to limit access to the Progress Editor just as with standard MFG/PRO menu programs:

- 1 Leave the Menu field blank.
- 2 Set Selection to 1.

- 3 Enter user IDs or groups for any users who should have access to the Progress Editor.

Another related control that should be considered is to disallow privileges for users connecting to the MFG/PRO database with a blank user ID. The Disallow Blank User ID Access option on the Progress Database|Admin|Security menu is available for this purpose.

Selecting this option denies all access privileges to the Progress blank User ID by placing a leading exclamation point (!) in each table and field permission specification for the database. See the next section for a more detailed description.

► See the “Maintaining Application Security” section in the Progress *Client Deployment Guide* for details.

Progress-Level Database Schema Controls

Progress-level security controls should also be considered for protecting the MFG/PRO database tables. Progress provides a schema security function to restrict various levels of access to specific database tables. This function is accessed from the Progress Data Administration|Admin|Security|Edit Data Security menu option.

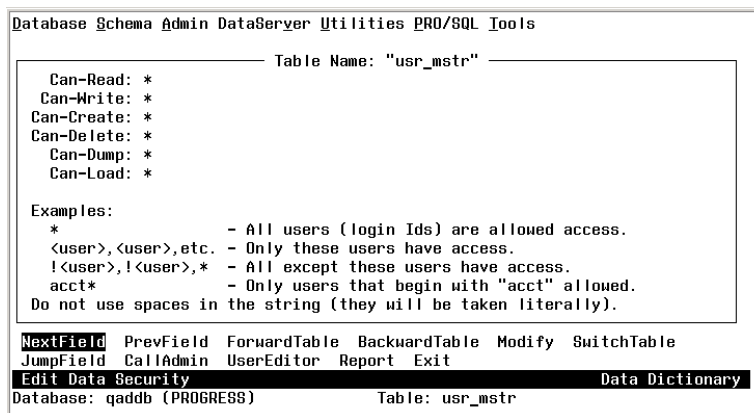


Fig. 7.3
Assigning Schema Controls

Select the NextField option to define access specifications at the individual field level as well.

These access specifications are enforced at compile time: Users are prevented from writing and executing custom source code in the Progress Editor if the code violates access restrictions.

Compiling Custom Code on Unprotected Databases

Progress schema-based controls do not prevent users from compiling code on an unprotected database with no schema-level access restrictions and then executing it on a production database. The schema access restrictions are checked at compile time rather than runtime.

► See the Progress Database Administration Guide for additional details on these functions.

To provide protection against this exposure, consider using the Progress PROUTIL function DBAUTHKEY to set a key for a Progress database.

Once set, this key is embedded in all r-code compiled against the database. In addition, any r-code is checked to verify that it contains this key value before it is permitted to execute. An additional function, RCODEKEY, is available to set or change the key value in specific r-code entries without recompiling source code.

Progress-Level Database Access

Unless properly controlled, it is possible under certain conditions to start a Progress session and then connect to an MFG/PRO database without starting the MFG/PRO application. After connecting, there would be no effective controls over accessing private or confidential data, modifying, or deleting records. Since an MFG/PRO session is never initiated, any application-level controls such as menu security could be circumvented. To mitigate this exposure, user and password access controls can be implemented at the Progress level as well as the MFG/PRO level.

To set Progress security, access the Edit User List option on the Admin|Security menu of the Progress Data Dictionary. Use this function to load valid user ID, name, and password combinations into the user security (_user) table.

Note Controls on user IDs and passwords that have been implemented for MFG/PRO do not apply to user records in the Progress _user table.

You can use this table in combination with command-line security options when the database is started. There are several possibilities:

- 1 No Progress users are defined and the `-U` and `-P` options are not specified. This is the default. The Progress user ID is set to the operating system log-in or the network log-in ID.
- 2 Progress users are defined but the `-U` and `-P` options are not specified. On all systems, this results in a blank Progress user ID. This can be used to establish basic system security for the majority of users. Any users with additional capabilities must specify a `-U` and `-P` at startup.
- 3 Progress users are defined and the `-U` and `-P` options are specified. The system verifies that the user ID and password combination is in the user security (`_user`) table. If not, an error displays and the session is not started.

Note If no Progress users are defined, the `-U` and `-P` options cannot be specified.

By setting Progress user/password controls on the MFG/PRO database, restricting access to the database files, and monitoring the database log file for unusual access events, security exposures from inappropriate access to the MFG/PRO database can be substantially reduced.

Workstation-Level Security

Depending on the operating system of the machines that are running MFG/PRO sessions, you may be able to combine an MFG/PRO security setting with operating system features to create an additional security layer at the workstation level.

The Timeout Minutes field in Security Control (36.3.24) lets you specify the number of minutes of inactivity that can occur before the system automatically logs a user out of an MFG/PRO session. Primarily used to reduce the system load resulting from users who stay logged in when they really do not need to be, this feature also enhances access security. If you set this to a reasonable number—such as 30—you can prevent users from inadvertently staying logged in when they go to lunch and leaving an open session that might be accessed by unauthorized individuals.

◆ See “Setting Up Security Control” on page 213.

For data integrity reasons—for example, to prevent a user from having a session terminated without saving modified data—this feature applies only when MFG/PRO is displaying a menu, rather than when a program is executing. To add workstation security for times when a user leaves a computer unattended while a program is running, you can use operating system features.

Windows Systems

Tip

This procedure assumes that users require passwords to access their computers.

In many environments, users run MFG/PRO on a Windows system; for example, GUI clients, character sessions using a terminal emulator, or QAD Desktop sessions using a Web browser. You can establish work procedures that require users to set up their machines to display a screen saver after a specified number of minutes and enter their Windows password—preferably not the same one used for MFG/PRO log-in—to turn off the screen saver.

♦ See the Windows online help for more information.

- 1 Right-click on the Windows desktop.
- 2 Select Properties.
- 3 Click the Screen Saver tab.
- 4 In the Wait field, enter the number of minutes that the machine is idle before the screen saver displays.
- 5 Select the box labeled On resume, password protect.
- 6 Click OK.

When the screen saver comes on, it can be cleared only when the current user's Windows password is entered, or when an individual with system administrator access overrides the user log-in.

Note Setting up this form of security does not affect any applications that are running when the screen saver displays—including MFG/PRO. It only blocks access to the computer.

Figure 7.4 illustrates an example of a computer running Windows XP set up for a 10-minute screen timeout, which can be cleared only by entering a password.

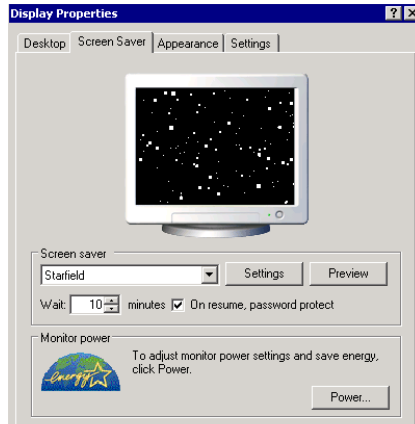


Fig. 7.4
Example of
Windows Screen
Saver Setup

To lock a computer manually without waiting for the screen saver timeout, press Ctrl+Alt+Delete, then click Lock Computer. A password is required to access a locked system. Your security policy should require users to do this when they leave their computers unattended as a matter of good security practice.

Note Depending on the operating system and version running on your Windows computers, as well as the way users are set up, the system administrator may be able to configure all machines in this manner and prevent individual users from changing the settings.

◆ See the operating system documentation for your system for information.

Non-Windows Systems

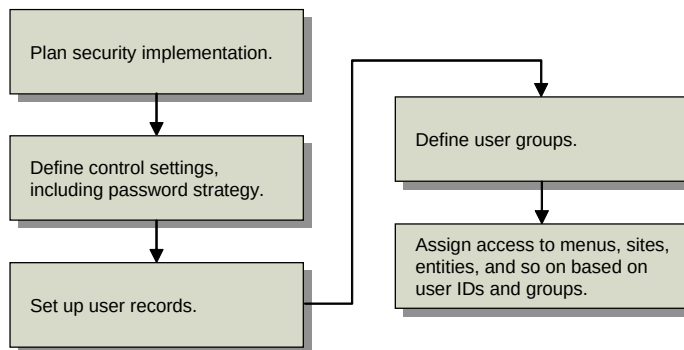
Many standard UNIX workstations—including those provided by HP, Sun, and IBM, which use the Common Desktop Environment (CDE)—offer screen-locking features much like those in Windows. Set up CDE-based machines using the Style Manager icon on the Front Panel. Similar features are also available for some LINUX environments.

◆ See the user documentation for your workstation for specific information.

Security Implementation Summary

Figure 7.5 illustrates a work flow for implementing and using the security features of MFG/PRO.

Fig. 7.5
Security Work
Flow



Establish a Security Plan

By default, only log-in security is defined in MFG/PRO. Once you set up explicit permission for one user to access entities, fields, menus, and so on, all other users are excluded. For this reason, you should have a comprehensive security plan before beginning to set up security records.

♦ See Table 7.1 on page 210.

The set of checklists provided in this chapter can serve as a starting point for determining the focal points to consider when establishing a plan.

You should consider both internal and external requirements when planning such security elements as password protection. For example:

- Does your company have specific requirements regarding password aging for all its systems?
- Do external regulatory agencies set standards for such things as password complexity, or whether the logged-in user ID should always display on the screen?
- Does your environment require database or operating system security controls implemented outside of MFG/PRO?

Other planning considerations apply if you are setting up security for a multiple-domain database.

For example, user profiles defined in User Maintenance apply to all domains in the system. However, profiles include several generalized codes that are domain specific such as access location and user type. To prevent validation errors, you should ensure that these codes exist in all domains.

◆ See “Defining Users” on page 223.

If you determine how you will use such system-wide data as part of your security planning effort, you can prevent duplication of effort by having basic information in place when you create new domains.

◆ See “Streamlining Setup” on page 57.

Additionally, be aware that while user IDs and groups are defined for the entire database, group security access is controlled on a domain-by-domain basis. For example, you can restrict a particular group from accessing a GL account in Domain 1—but give the same group access to that account in Domain 2.

Implement Your Security Plan

After planning how your security system should operate to meet your company’s specific requirements, perform the following tasks to implement the plan:

- Define control settings using Security Control (36.3.24). An important feature of this program is the Passwords frame, where you establish a system-wide password strategy.
- Set up user records. Depending on your overall security plan, you can define such elements as domain access and group membership, as well as enter temporary passwords for your users.

◆ See page 213.

◆ See page 223.

Note If you want to assign users to groups at the same time you set up user records, you must define groups first. Alternatively, you can just define the users and assign them to groups in User Group Maintenance (36.3.4).

- Based on how you want to control access to MFG/PRO functions, define groups using User Group Maintenance.
- Use several programs to set up user or group access to menus, fields, sites, entities, GL accounts, and inventory movement codes.

◆ See page 235.

◆ See page 238.

Security Planning Checklists

Tables 7.1 through 7.3 summarize the various security controls that should be considered as part of an effective overall information security plan for MFG/PRO. The degree to which each of these items is relevant will be a function of an organization's security requirements.

Where applicable, the tables include references to information on related topics.

Table 7.1
Planning, Policies,
and Procedures
Checklist

Topic	Reference
Review all information security documentation for both MFG/PRO and Progress prior to installation (or software upgrade if applicable).	• This chapter • MFG/PRO <i>Installation Guide</i> • <i>Installation Guide: Enhanced Controls</i> • Progress documents, including <i>Data Administration, Guide, Client Deployment Guide, and Programming Handbook</i>
Review all MFG/PRO-related files to determine the appropriate permission and ownership settings.	"Operating System and Progress Security" on page 201
Document the users who should be permitted access to MFG/PRO and verify user IDs.	"Defining Users" on page 223
Determine if user groups will be used, and if so document the group names and the user IDs to be assigned to each group.	"Controlling Access with User Groups" on page 234
Consider requirements for policies and/or procedures regarding deactivation of old user accounts. To meet the requirements of many regulated environments, user accounts can be deactivated, but not deleted, once they have been used to access the system.	"Defining Users" on page 223
Define policies and procedures to be used to assure that user and group membership information will be kept current.	
Determine procedures to be used to create new user accounts and communicate initial passwords (e-mail, personal contact, other).	"Create a Password Strategy" on page 219
Decide if a simplified access approach is sufficient. This lets users log in based on operating system-level security.	"OS-Based Log-in Security" on page 200

Topic	Reference
Define how often users are required to changed passwords, and update the corresponding MFG/PRO security setting.	“Expiration Days” on page 221
Define procedures for failed log-ins, including: • The number of failed attempts before an event notification should be communicated to the defined security administrators • Alternatives to e-mail notification • Reviews of system logs • Procedures for resetting locked accounts	• “Setting Up Security Control” on page 213 • “Monitoring System Security” on page 250
Define password policies and procedures, including password composition, length, expiration, and reuse of previous passwords.	“Create a Password Strategy” on page 219
Define appropriate policies and procedures for users requiring that MFG/PRO sessions be locked using a screen saver or comparable mechanism whenever the user leaves the session unattended.	“Workstation-Level Security” on page 205

Topic	Reference
Determine whether to implement Progress as well as MFG/PRO user ID and password controls.	“Progress-Level Database Access” on page 204
Determine requirements for Progress-level schema security to control access to MFG/PRO database tables.	“Progress-Level Database Schema Controls” on page 203
Consider disallowing Progress-level table and field access for the blank user ID	“Progress Editor Access” on page 202
Determine the period of inactivity after which an MFG/PRO session should be disabled. For each device used to access MFG/PRO, assure that a screen saver, or comparable utility, is set to activate after the defined period of activity, requiring reentry of the user’s password to unlock the MFG/PRO session.	“Workstation-Level Security” on page 205
Determine whether multiple users share a common workstation to access MFG/PRO and whether appropriate operating system functionality exists to adequately support security.	Operating system documentation

Table 7.2
Progress and
Operating System
Checklist

Table 7.3
MFG/PRO Security
Parameters, Setup,
and Processes
Checklist

Topic	Reference
Verify and update relevant MFG/PRO control program settings, especially those for security.	“Setting Up Security Control” on page 213
Review any currently defined users and groups in MFG/PRO and disable any inappropriate, inaccurate, or out-of-date entries.	“Controlling Access with User Groups” on page 234
Define users designated as security administrators, who will receive e-mail notification of security events such as failed log-ins exceeding a defined threshold.	• “Administrator Group” on page 217 • “Maximum Access Failures” on page 216
Update MFG/PRO security settings regarding user IDs and passwords, including: • Password composition • Password length • Password expiration • Limits on re-use of previous passwords • Limits on number of failed logon attempts	“Create a Password Strategy” on page 219
Determine how MFG/PRO security functions should be implemented to protect the integrity of database records. For each menu item, site, GL account, and so on, specify the appropriate users or groups authorized to execute the menu program or access data.	“Using Security Functions” on page 238
Review menu function authorizations for potential segregation of duty issues and adjust groups as appropriate.	“Controlling Access with User Groups” on page 234

Security Programs

Table 7.4 lists the menu programs you use in defining and maintaining security for your system.

Table 7.4
System Security
Menu (36.3)

Number	Description	Program
36.3.1	User Maintenance	mgurmt.p
36.3.2	User Inquiry	mguriq.p
36.3.3	User Password Maintenance	mgurmt.p
36.3.4	User Group Maintenance	mgurgpmt.p
36.3.5	User Group Inquiry	mgurgpiq.p
36.3.10	Menu Security Maintenance	mgpwmt.p
36.3.11	Menu Security Change	mgpwcg.p

Number	Description	Program
36.3.13	Entity Security Maintenance	glsecmt.p
36.3.14	Entity Security Inquiry	glseciq.p
36.3.15	Site Security Maintenance	clsismt.p
36.3.16	GL Account Security Maintenance	mgacsmt.p
36.3.17	Inventory Movement Code Security	sosimt.p
36.3.18	Inv Mvmt Code Security Browse	gpbr502.p
36.3.19	Field Security Maintenance	mgflpwmt.p
36.3.20	Field Security by Group	mgflgpmt.p
36.3.22	User Access by Application Inquiry	lvusriq.p
36.3.23	Reports and Utilities Menu	
36.3.23.1	Logon Attempt Report	mgurpsrp.p
36.3.23.2	User Account Status Report	mguactrp.p
36.3.23.4	User Group Report	mgurgprp.p
36.3.23.12	User Password Force Change Util	utfrcpw.p
36.3.23.13	Entity Security Report	glsegrp.p
36.3.23.15	Site Security Report	clsisrp.p
36.3.23.16	GL Account Security Report	mgacsrp.p
36.3.23.19	Activated Field Security Report	mgflpwrp.p
36.3.23.20	Dictionary Field Security Report	mgfldcrp.p
36.3.24	Security Control	mgurpmmt.p

Setting Up Security Control

Use the two frames of Security Control (36.3.24) to:

- Establish basic security parameters for your environment
- Define the way you want to set up and control passwords

Two special security considerations apply to records created in this program:

- Whenever a field is updated, the system notifies members of the administrator group by e-mail.
- You must use this program to update data values in the user control (usrc_ctrl) table. The system prevents you from using other methods, such as Progress Editor, to modify that record.

◆ See page 222.

Fig. 7.6
Security Control
(36.3.24), Initial
Frame

Session ID Prefix. Enter a prefix for temporary system-generated work files. These are created in the directory where the user started MFG/PRO. The default is TMP. Modify this field only if you access multiple databases from the same directory. If the prefix in both databases is TMP, one session's temporary files could overwrite another's.

Timeout Minutes. Specify a number of minutes after which the system should automatically log out inactive sessions. Set a value in this field to minimize unnecessary overhead on busy systems.

See
"Workstation-
Level Security"
on page 205.

The field can also be used as part of an overall security strategy to prevent users from inadvertently allowing access to unauthorized individuals.

If you enter a value, the system considers a session inactive only when a menu is displaying. If the user is in a menu function—Item Master Maintenance, for example—a session is never automatically logged out.

See *User Guide*
Volume 9:
Manager
Functions for
details on
licensing.

Enforce Licensed User Count. Use this field to implement enforcement of the total number of users, sessions, or transactions allowed based on your license agreement.

No (the default): The system issues license violation warnings if you violate your license agreement, but you are not prevented from completing the action that caused the violation.

Yes: The system issues a violation error if you violate your license agreement and you cannot complete your current activity.

The system tracks all license violations, both warnings and errors. License violations can occur in the following situations:

- In User Maintenance (36.3.1) when you attempt to add users or assign them to applications
- In License Registration (36.16.10.1) when you assign users to applications
- During user log-in to the system
- When users attempt to use separately licensed applications or nonregistered applications

Important Violation warnings should not occur often; if repeated warnings occur, contact your QAD representative or distributor for a license upgrade.

Enforce OS User ID. Specify whether the system allows users to access MFG/PRO character and Windows sessions based on their operating system log-in.

◆ See “OS-Based Log-in Security” on page 200.

No: Users are always required to enter a valid user ID and password.

Yes: Depending on password parameters defined in Security Control, valid MFG/PRO users may be able to access the system directly without entering log-in information.

Header Display Mode. Use this field to control the information that displays in the menu and program title bars of MFG/PRO programs in the character and Windows user interfaces.

Note Display mode does not affect the display of programs in QAD Desktop. Desktop programs always show the domain short name and currency in the program title bar. Additionally, the browser title bar shows the full user name associated with the user ID, the log-in domain name, and the database name.

Valid values are:

0 (Display Date). The menu title bar displays the name associated with the ~SCREENS address code defined in Company Address Maintenance (2.12) and the current database name defined in Database Connection Maintenance. The program title bar from left to right includes the program name, the version of the program, the menu number and title, and the current date (see Figure 7.7).

Fig. 7.7
Display Mode 0

sosomt 99	7.1.1 Sales Order Maintenance	07/17/03

1 (Display User ID). The menu title bar is the same as choice 0. The program title bar is the same as choice 0 except that the log-in ID of the current user replaces the current date. Reading from left to right, the title bar includes the program name, the version of the program, the menu number and title, and the log-in ID of the current user (see Figure 7.8).

Fig. 7.8
Display Mode 1

sosomt 99	7.1.1 Sales Order Maintenance	hme

2 (Display Date with Domain). The menu title bar displays only the current database name defined in Database Connection Maintenance. The program title bar from left to right includes the short name and currency of the current working domain, the menu number and title, and the current date (see Figure 7.9).

Fig. 7.9
Display Mode 2

Head Office	[USD] 7.1.1 Sales Order Maintenance	07/17/03

3 (Display User ID with Domain). The menu title bar is the same as choice 2. The program title bar is the same as choice 2 except that the log-in ID of the current user replaces the current date. Reading from left to right, the program title bar includes the short name and currency of the current working domain, the menu number and title, and the log-in ID of the current user (see Figure 7.10).

Fig. 7.10
Display Mode 3

Head Office	[USD] 7.1.1 Sales Order Maintenance	hme

♦ See “Using Ctrl+F to View Information” on page 71.

Note Some regulatory environments may require the name associated with the user ID of the logged-in user to be available from any program. In the character and Windows interfaces, you can use the Ctrl+F key combination to review this information and other context details. In QAD Desktop, the user name displays by default in the browser title bar, along with the current domain and database name.

♦ See “E-Mail Notifications” on page 222.

Maximum Access Failures. Enter the maximum consecutive failed log-in attempts allowed before the system deactivates the user’s log-in ID. When an account is deactivated, the system sends an e-mail message to members of the specified Administrator Group.

Leave this field set to zero (0) if you do not want to limit failed access attempts.

Note If you are using electronic signatures, this same value controls the number of failed signature attempts that are allowed before the system deactivates the user ID.

◆ See “Recording Electronic Signatures” on page 316.

Administrator Group. Designate a user group—defined in User Group Maintenance—as an administrator group. Group members receive e-mail notifications when specific security and controlled events occur; for example:

- When a user account is deactivated for too many failed log-in attempts ◆ See page 222.
- If you are using audit trails, when an audit trail profile is activated or an error occurs during the audit trail creation process ◆ See page 280.
- If you are using electronic signatures, when an electronic signature profile is activated or a user account is deactivated for too many failed signature attempts ◆ See page 321.
- When an update is made in Security Control ◆ See page 222.

Typically, this group includes the primary system administrator and one or more alternates.

Email System. Specify an e-mail system definition—set up in E-Mail Definition Maintenance (36.4.20)—used to notify members of the administrator group when security and Enhanced Controls events take place.

◆ See *User Guide Volume 9: Manager Functions* for information on e-mail.

Note The system first attempts to use the e-mail definition specified for the logged-in user in User Maintenance. If the user record does not include a valid e-mail definition, the one specified in this field is used.

Important For system-generated e-mail to work correctly, be sure that the e-mail system definitions specified both here and for individual users are based on a message text *file*, rather than a message text *string*, in E-Mail Definition Maintenance.

Additionally, if you use the MFG/PRO Windows user interface, the system uses the e-mail program on the client machine to send security-related e-mail. This means that a Windows e-mail program must be

installed on each client machine. For example, if you use `wMailTo.exe`, that program must be installed and configured in the MFG/PRO home directory on each client.

Logon History Level. Indicate the level of system-maintained log-in history.

None (the default): Log-in history is not maintained.

Failed: Log-in history is maintained only for failed log-in attempts.

All: History is maintained for all log-in activity.

◆ See “Monitoring System Security” on page 250.

Particularly in highly regulated security environments, you can use log-in history information as part of an overall access monitoring effort. Use Logon Attempt Report (36.3.23.1) to view log-in history.

Note Be sure to set this field based on the level of information you think will be needed when you run the report. For example, if you set the history level to None, Logon Attempt Report will not include any data.

◆ See *User Guide Volume 9: Manager Functions* for more information on reason codes.

Active Reason Type. This is a display-only field. The system-assigned value is `USER_ACT`, the reason type associated in Reason Codes Maintenance (36.2.17) with reason codes used by security functions. The system uses reason codes of this type in two places:

- The Auto-Deactivation Reason field
- Reason codes entered manually in the Active Reason field in User Maintenance

◆ See “Active Reason” on page 229.

Example You could use Reason Codes Maintenance to create the following reason codes associated with type `USER_ACT`:

- `AUTO`. The system automatically deactivated the account. You could enter this in Auto-Deactivation Reason.
- `REACT`. The system administrator has manually reactivated the account.
- `NEW`. The system administrator has added the account for a new user.
- `LEFT`. The user is no longer with the company, and the system administrator has deactivated the account.

Note System installation or conversion automatically creates one default reason code, QAD_DEF, for reason type USER_ACT. After installation, this code displays in the Active Reason field in the User Maintenance record of the default system user. During conversion, existing user records are populated with this value. After you set up values in Reason Codes Maintenance that apply to your system, you do not have to use this default reason code.

Auto-Deactivation Reason. Enter the reason code the system enters in user records when it automatically deactivates a user account. This occurs when the user reaches the number of consecutive failed log-in attempts specified in Maximum Access Failures. This code must be defined in Reason Codes Maintenance and be associated with reason type USER_ACT.

Important Reason codes are domain specific. During security planning, you should determine the codes you will use and set them up as part of the system domain. This way they are copied by default to all new domains.

Create a Password Strategy

Use the Password frame to define the complexity requirements and expiration time period for user account passwords. Anytime a new password is created for an account—either manually or automatically—that password must meet the rules you set up here. Use as many or as few password parameters as required by the security guidelines set for your environment.

If you enable automatic password creation by setting Password Creation Method to Email or Display, the system uses the parameters you specify to generate new passwords.

If you choose to allow valid users to access MFG/PRO based directly on operating system security, do not define any password parameters; set Enforce OS User ID to Yes in the initial frame of Security Control. To default the user ID from the operating system but still require an MFG/PRO password at log-in, set that field to Yes and specify password parameters as needed.

◆ See “OS-Based Log-in Security” on page 200.

Fig. 7.11
Security Control,
Password Frame

Password	
Minimum Length:	3
Min Numeric Characters:	1
Min Non-Numeric Characters:	1
Minimum Reuse Days:	1
Minimum Reuse Changes:	1
Password Creation Method:	No
Password Expiration Days:	0
Warning Days:	0

Minimum Length. Enter the minimum number of characters allowed for new passwords. Password cannot exceed 16 characters. Leave the default 0 (zero) to indicate that a blank password is allowed.

▶ See page 250.

Note Passwords are validated against structure requirements only when they are first created, rather than each time they are used. To make password structure changes apply immediately, use User Password Force Change Utility (36.3.23.12) to force users to change their passwords at the next log-in. New passwords must meet the updated structure requirements.

Min Numeric Characters. Enter the minimum number of numeric characters required for new passwords. This value plus the value in Min Non-Numeric Characters cannot exceed 16 and must be the same as or less than the specified minimum length. Leave the default 0 (zero) to indicate that numeric characters are not required in the password.

Min Non-Numeric Characters. Enter the number of non-numeric characters required for new passwords. This value plus the value in Min Numeric Characters cannot exceed 16 and must be the same as or greater than the specified minimum length. Leave the default 0 (zero) to indicate that non-numeric characters are not required in the password.

Minimum Reuse Days. Indicate the number of days a user must wait before a password can be reused. The system maintains all user passwords for historical purposes. If users define new passwords at specific time intervals, you can set this value so that the same password is not reused for a specific period of time.

Example Enter 364 to indicate that users cannot select a password already used in the previous year.

This password check can be used independently or in conjunction with the next field, Minimum Reuse Changes. If you set both options, both rules apply. Leave the default 0 (zero) to indicate that this rule should not apply.

Minimum Reuse Changes. Indicate the number of password changes required before a password can be reused. The system maintains all user passwords for historical purposes. You can set this value so that the same password is not reused until the user has changed their password at least this many times.

Example Enter 3 to indicate that users must change their passwords three times before they can use the same password again.

This password check can be used independently or in conjunction with Minimum Reuse Days. If you set both options, both rules apply. Leave the default 0 (zero) to indicate that this rule should not apply.

Password Creation Method. Specify the method you want to implement for creating new temporary passwords:

- No (the default). The system administrator must define temporary passwords manually. Automatic password generation is not enabled.
- Display. A new temporary password is automatically generated and displayed on the screen in User Maintenance. The system administrator must then communicate it to the user.
- Email. A temporary password is automatically generated and e-mailed to the address defined in User Maintenance for the user ID. This method is especially useful in high-security environments because the user is the only person who has access to the temporary password.

◆ See “Updating Passwords” on page 230.

◆ See “E-Mail Notifications” on page 222.

Note All passwords created using the specified method are temporary, single-use passwords. The user is forced to change this password at the first log-in.

Expiration Days. Specify the number of days users can use the same password before the system prompts them for a new one.

Once the specified number of days passes since a user’s last password change, they are prompted for a new password at the MFG/PRO welcome screen. When this field is 0 (zero), passwords never expire.

Note The date of the user's last password change displays in User Maintenance and User Password Maintenance.

Warning Days. Enter the number of days before a password will expire when users are warned of the upcoming expiration date. This must be less than the value of Expiration Days.

Users are reminded of the expiration date at each subsequent log-in and can optionally update their passwords immediately or, depending on menu access, update them in User Password Maintenance.

E-Mail Notifications

Based on Security Control settings, the system can automatically send e-mail to users in the following security-related situations:

- When a user's consecutive number of failed log-in attempts exceeds the number specified in Security Control, the system generates and sends e-mails to the specified administrator group. The e-mail text is similar to the following:

The purpose of this email is to inform you that a user has been deactivated for exceeding the maximum logon failures allowed as setup in Security Control. You have been included in this email distribution because you belong to the Administrator group identified in Security Control for MFG/PRO.

User ID deactivated for exceeding max logon failures allowed: *User ID*

This e-mail was automatically generated from an MFG/PRO process. If you have any questions about this e-mail, contact the MFG/PRO system administrator. Do not reply to this e-mail.

- When Password Creation Method is set to E-mail in the Password frame of Security Control, the system generates a new password and e-mails it to the user based on the e-mail address specified in User Maintenance. This occurs for new and existing users when Update Password is Yes in User Maintenance. The e-mail text is similar to the following:

The purpose of this e-mail is to inform you of your new temporary MFG/PRO password. You have been sent this e-mail because Security Control has been set up to e-mail autogenerated temporary passwords.

Your temporary MFG/PRO password is: *password*.
You will be forced to change this password at next logon.

This e-mail was automatically generated from an MFG/PRO process. If you have any questions about this e-mail, contact the MFG/PRO system administrator. Do not reply to this e-mail.

- When any field is updated in Security Control, the system generates and sends e-mails to the specified administrator group. The e-mail text is similar to the following:

The Security Control menu program has been used to change the security configuration of MFG/PRO. Please review this information carefully to ensure that these changes will not compromise the system security. You have received this email because you belong to the Administrator group identified in Security Control for MFG/PRO.

Changes made by user: jnw

Changed Field: old, new

=====

Administrator Group: 200401170000219243.4321,
200312090000112641.4321

Password Expiration Days: 99, 0

Logon History Level: 2, 1

Maximum Access Failures: 99, 0

Header Display Mode: 1, 2

Enforce OS User Id: yes,

This email was automatically generated from an MFG/PRO process. If you have any questions about this email, contact the MFG/PRO system administrator. Do not reply to this email.

Note Values shown in this message are those stored in the database and may not be the same as displayed in the user interface. For example, the Administrator Group values display as the unique object identifier (OID) codes associated with the old and new values in the database. The message is intended primarily to show administrators which fields were changed.

Defining Users

You define users by assigning a unique ID in User Maintenance (36.3.1). Each program is always passed the user's ID, any group names associated with the user for the current domain, and access information associated with the user. After you create the ID for a user, you specify other identifying information and preferences.

Tip

User IDs cannot be blank, or the same value as a user group name.

Fig. 7.12
User Maintenance
(36.3.1)

◆ See “Basic Log-In Security” on page 198.

To log in to MFG/PRO, each user must specify a unique user ID and the associated password. Other user data is referenced throughout MFG/PRO and may be required for reasons other than security.

User profiles apply to all domains in the system. However, profiles include several generalized codes that are domain specific such as access location and user type. To prevent validation errors, you should ensure that these codes exist in all domains.

Note Batch processes must be assigned a valid user ID.

Tip
This restriction ensures a complete audit trail of users who have accessed the system.

Once a user has accessed the system, the ID cannot be deleted. Instead, you can make users inactive. If an ID has never been used for log-in, you can delete it, if necessary. This lets you correct any errors made during initial setup.

Interaction with Licensing

◆ See *User Guide Volume 9: Manager Functions* for details on licensing.

There are three license types for MFG/PRO: named user, concurrent session, and business process cycle, which is used in combination with named user licensing. Concurrent session licensing is checked at log-in. Named user licensing is verified in User Maintenance.

For a named user license, the system counts the number of active users authorized to access the licensed application and compares the number against a predefined limit for the license.

If the number of active users exceeds the predefined limit specified in the license agreement, a violation message displays in User Maintenance. Violation messages can be either warnings or errors, depending on

whether enforcement of the license policy is implemented. Errors prohibit actions in User Maintenance when the limit on license agreements is reached; warnings allow actions to continue.

System administrators can implement enforcement of license agreements by setting the Enforce Licensed User Count field to Yes in Security Control (36.3.24). Setting this field determines whether:

► See “Setting Up Security Control” on page 213.

- Errors or warnings display in User Maintenance.
- System administrators can create new users when the number of existing users exceeds the licensed number.
- Additional users can log in when the number of sessions exceeds the licensed number.

The applications a user can access must be activated for the user. You can activate access to applications here or when you register an application license code in License Registration (36.16.10.1). This includes the base MFG/PRO application. If a user ID is obsolete, you should inactivate access to all registered applications.

Controlling Information Process and Display

You can ensure that MFG/PRO data is correctly displayed and processed for a given user—regardless of the user’s language or location—by specifying the following values in User Maintenance:

Language. Enter a two-letter code identifying the user’s language. The system displays menus, messages, and other interface elements in this language when the user logs in.

Country Code. Enter a three-character country code to associate with the user. The country code must be defined in Country Code Maintenance (2.14.1) and it must have an associated alternate country code.

► See *User Guide Volume 6: Master Data*.

The alternate country code must be a valid International Organization for Standardization (ISO) country code. The system uses the ISO code to set up date and number formats and other interface elements for each user session.

Variant. Optionally enter the locale for the user. This field can be used to specify regional variations within a country.

♦ See the installation guide for more information.

Information on language, country code, and variant are maintained in a file named `locale.dat`, along with other format information. Once the system determines a user's language, country code, and corresponding ISO country code, it gets information from `locale.dat` and uses it to set user-specific date and number formats.

System administrators may need to change information in `locale.dat` or add entries for countries that are not included in the current file.

Each line in the file follows the same format. For example, the line for US English looks like this:

```
US,en,US,,mdy,American
```

Where:

- US is the MFG/PRO language code.
- en is the ISO language code.
- US is the ISO country code.
- Optional variant is blank.
- mdy is the date format.
- American is the numeric format (period as the decimal separator; comma as the thousand separator).

Identifying Users

Use the following fields to identify this user:

User Type. Enter the type associated with this user.

- Employee identifies internal users who are employees.
- Customer identifies external customers who are authorized to access the system remotely. To assign a customer type to a user, you must enter a valid customer ID as the user ID in User Maintenance.
- QAD identifies QAD employees who do customer support or service work.
- API identifies users who access MFG/PRO through an application programming interface connection.

Employee is the default for all newly created users except customers. When you enter a customer ID as the user ID, the type defaults to customer.

You may need to define additional types if users do not fit into the four categories; for example, you may need a contractor or part-time type. You must predefine the new user type in Language Detail Maintenance (36.4.3) before you can assign it to users here.

Time Zone. Enter a time zone to associate with this user. Time zones must be predefined in Multiple Time Zones Maintenance (36.16.22.1). Time zone defaults from the server time zone specified in Database Control (36.24).

◆ See “Setting a Default Time Zone” on page 67.

Remark. Use this field to enter a brief text comment regarding the user. For example, you could note that this user is currently on leave of absence and the ID has been deactivated.

Specifying E-Mail Addresses

Associate a valid e-mail address and definition with each user who receives messages generated by MFG/PRO.

◆ See *User Guide Volume 9: Manager Functions* for details on e-mail setup.

E-mail can be used with many MFG/PRO features. For example:

- System administrators can receive automatic notification when user IDs are deactivated because of log-in violations.
- Based on a Security Control setting, users can receive system-generated passwords by e-mail.

Note If you plan to use this feature, be sure to specify e-mail data when you set up user accounts so that users can receive their passwords.

- Enhanced Controls uses e-mail to inform administrators of unusual audit trail and electronic signature events.

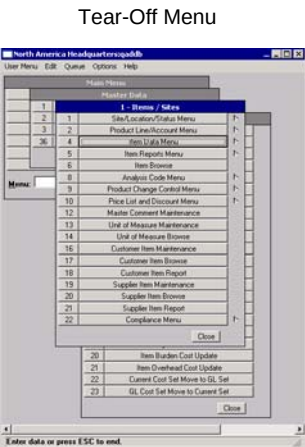
Setting Interface Preferences

▶ See *User Guide Volume 1: Introduction* for more information on the user interface.

Select interface preferences for individual users by specifying values for the following:

- Whether menu substitution is enabled or disabled. This only affects menus in Windows and character sessions. This does not affect the Desktop interface, where menu substitution is assumed to be always on.
- Menu style. This only affects the menu style used in an MFG/PRO Windows session.
 - The icon menu style has large buttons that lead you into the different parts of the system and show a hierarchy of your location in a submenu.
 - The tear-off menu style enables you to choose your menu layout.
 - The character-based menu style emulates traditional character terminals.

Fig. 7.13
Menu Style Options
(GUI Interface
Only)



Character Menu



Icon Menu



Specifying Security Settings

Use the System Access frame to specify security-related access settings for each user.

The screenshot shows a 'System Access' frame with the following details:

- Active:** ☒ (Yes)
- Active Reason:** new
- Force Password Change:** ☐ (No)
- Update Password:** ☒ (Yes)
- Last Logon:** 12/10/2003 08:24 PST/PDT
- Last Password Change:** 12/01/2003
- added user** (text label)

Fig. 7.14
User Maintenance,
System Access
Frame

Active. Indicate whether this user ID can be used to log in to the system. To deactivate an existing user ID, enter No.

Note Anytime this field is updated, the Active Reason field must also be updated.

Active is updated in the following ways:

- Automatically when you enter a new user ID. By default, the system sets Active to Yes; you must manually enter an active reason.
- Automatically when the system deactivates an account for too many failed log-in attempts. Active Reason is set to the code specified in Security Control.
- Manually when you update an existing ID; for example, you can do this to reactivate a system-deactivated user record, or to deactivate an account when a user leaves the company. You must enter an active reason.

▶ See “Maximum Access Failures” on page 216.

Inactive accounts do not display in most user lookups.

Once a user ID has been used for log-in, it cannot be deleted from the system. If an ID is no longer needed, deactivate it.

Active Reason. Enter a reason code that indicates the reason for modifying the setting of Active. This reason code must be associated with reason type USER_ACT.

▶ See “Active Reason Type” on page 218.

You must update this field anytime you change the Active field.

Access Location. Enter a code that associates the user with a major business facility or major business location. If you have more than one facility or location or if users work remotely or in small offices, associate the user with the major business facility or location that is most appropriate.

Access location codes must be defined in Generalized Codes Maintenance (36.2.13) for field `usr_access_loc`. MFG/PRO ships with a Primary location code that is used as the default for new user records. You can use this location as your company home office location or central processing site.

Force Password Change. Indicate whether the system should force this user to create and validate a new password the next time they log in to the system using the current password.

The default is Yes for new users and cannot be updated. This lets you assign temporary, single-use passwords either automatically or manually.

The field defaults to No for existing users unless the password has been changed. In that case, it is set to Yes and you cannot update it. This forces users to assign their own passwords at the next log-in.

Use Force Password Change Utility (36.3.23.12) to set this field to Yes for selected users or user groups.

Update Password. Specify whether this user requires a new password. For new users, the field defaults to Yes and you cannot change it.

Updating Passwords

♦ See “Create a Password Strategy” on page 219.

When Update Password is Yes in the System Access frame, subsequent actions depend on the setting of Password Creation Method in Security Control:

- Display. The system-generated password displays at the bottom of the screen.
- Email. The system generates a password and e-mails it to the user.
- No. Automatic password generation is disabled. A frame displays for you to manually enter a new password.

Note Passwords specified in User Maintenance are single-use, temporary passwords generated by the system or entered by the system administrator. At log-in, the user is prompted to enter a new password.

Fig. 7.15
User Maintenance,
Set New Password
Frame

Enter a new password. Since the system does not display passwords, type it again to confirm it.

Note The new password must conform to structure and reuse rules defined in Security Control.

Passwords expire based on the value of Expiration Days in Security Control. If you want to let users change their own passwords at a time other than log-in, give them access to User Password Maintenance (36.3.3).

▶ See “Expiration Days” on page 221.

Specifying Domains

Use the domain frame to enter or update the domains to which this user has access. If you specify more than one domain, identify the one the system uses as the default at log-in. Additionally, you can enter or update the user groups that control security access for the user while in this domain.

▶ See “Shared-Services Domain” on page 11 for an overview of domains.

Domain	Name	Default	Database
matdom	material	☐	QADDB
QAD	System Domain	☒	qadddb

Domain: st92brmfg qad.inc Default: ☒

Update Groups:

Fig. 7.16
User Maintenance,
Domain Frame

Domain. Enter the code identifying a domain this user can access. The domain name displays next to the code.

The functions that the user can execute in this domain are determined by access granted to the groups associated with the user in this domain. Set Update Groups to Yes to enter or update the list of user groups associated with this user in this domain.

Default Domain. Enter Yes if this is the user's default domain; otherwise, enter No. This field defaults to Yes for the first domain assigned to a user.

Note In a multiple-database environment, a user's default domain must be associated with the current database; it cannot be a connection record.

When a user logs in to an MFG/PRO database, the system retrieves the information associated with the user in User Maintenance. In the character and Windows UIs, a user with access to more than one domain is prompted for a domain code, which defaults from the record marked as default.

A user with only one assigned domain does not see this prompt at log-in but is automatically logged in to the single domain associated with the ID specified.

Only one domain can be designated as default. When you enter Yes, the system verifies if another default domain exists for the user. If it does, a warning displays and you are prompted to continue. If you choose to continue, the current domain becomes the default and the system no longer uses the other domain as the default during log-in.

You cannot exit this frame without assigning a default domain to the user. An error is generated and you are prompted to continue. If you continue, any changes made in the current session are discarded.

♦ See "Changing the Current Domain" on page 63.

A user with access to multiple domains can use Change Current Domain (36.10.13) to switch to another domain at any time during an MFG/PRO session. Otherwise, all session activity takes place in the domain specified at log-in.

Update Groups. Enter Yes to display a frame that lets you enter or update the list of user groups associated with this user in this domain. Groups are required only if you control security access by group. Set this field to No to skip the group frame for this domain.

♦ See "Defining User Groups" on page 235.

Note You also can associate users with groups in each domain in User Group Maintenance (36.3.4).

Specifying User Groups

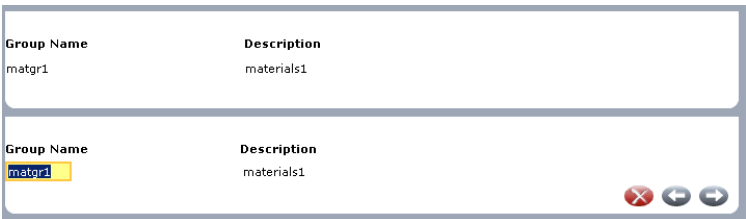
Group membership can determine whether a user is given access to menus, sites, and other system elements. The system always considers the user's ID and any group names associated with the user for the current domain when allowing access to various functions.

▶ See “Controlling Access with User Groups” on page 234.

Use groups to streamline security setup. Many users can belong to a single group; when a new user record is created, you can add the user to existing groups to ensure they have correct access.

When Update Groups is Yes in the domain frame, the system displays a list of all the groups currently assigned to the user for the domain. Use the Group Name field to add groups, or press Delete to remove them.

Note Groups must be defined in User Group Maintenance (36.3.4) before you can enter them here.



Group Name	Description
matgr1	materials1

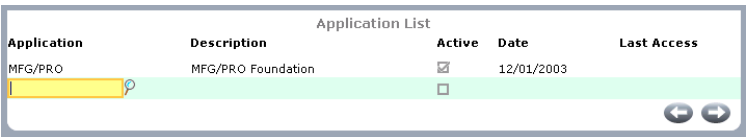
Group Name	Description
matgr1	materials1

Navigation icons: [X] [Left Arrow] [Right Arrow]

Fig. 7.17
User Maintenance,
Group Frame

Specifying Application Use

The Application List frame in User Maintenance lets you define the software applications that a user can access. When you define a new user, the system prompts you authorize the new user for all licensed applications. If you respond Yes, Active is set to Yes for all licensed applications for this user. Otherwise, MFG/PRO is listed as the only active application. You can list additional licensed software applications, then set Active to Yes or No for each application. The default is Yes.



Application	Description	Active	Date	Last Access
MFG/PRO	MFG/PRO Foundation	☒	12/01/2003	
		☐		

Navigation icons: [Left Arrow] [Right Arrow]

Fig. 7.18
User Maintenance,
Application List
Frame

♦ See “Interaction with Licensing” on page 224.

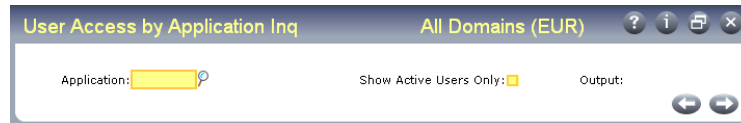
The application name you enter under Application Name must be registered with MFG/PRO through License Registration (36.16.10.1).

You can also specify which users can access an application after you register the application in License Registration.

If you deactivate MFG/PRO for a user, all other registered applications are deactivated, too.

Use User Access by Application Inquiry (36.3.22) to view a list of applications as well as the user’s ID and name, active or inactive status of each application, time zone, access location, and access date.

Fig. 7.19
User Access by
Application Inquiry
(36.3.22)



Controlling Access with User Groups

MFG/PRO lets you assign users to groups, then control access to various system elements based on group membership. This feature provides flexibility and consistency in the way you enforce security requirements.

♦ See *User Guide: QAD Desktop* for information.

Important A group security feature is also available in QAD Desktop. However, this is supported by a different set of records than standard MFG/PRO user groups.

First, define groups in User Group Maintenance (36.3.4). Then use the following programs to assign access based on groups:

- ♦ See page 240.
 - Menu Security Maintenance (36.3.10)
- ♦ See page 246.
 - Site Security Maintenance (36.3.15)
- ♦ See page 248.
 - GL Account Security Maintenance (36.3.16)
- ♦ See page 249.
 - Inventory Movement Code Security (36.3.17)

♦ See “Specifying Domains” on page 231.

When a user is given access to more than one domain, you can use groups to manage roles within the domain.

Example A user has access to all functions in Domain1, but can only generate reports in Domain2. Assign the user to two groups: Admin and Review. Set up menu security so that Admin can access all functions and Review can access only reports. Then, in User Maintenance, assign the user to the Admin group for Domain1 and to the Review group for Domain2.

Grouping users reduces maintenance for the system administrator.

For most security, the use of groups is entirely appropriate. In a few cases, you might not want to use groups. For high-risk functions such as Menu Security Maintenance, grant access to specific users by ID—typically the system administrator and an alternate.

Defining User Groups

Use User Group Maintenance (36.3.4) to create groups that can be used to control access to various aspects of MFG/PRO and associate them with domains and users.

Two administrative user groups are required in the system:

- The administrator group specified in Security Control (36.3.24) to receive e-mail notifications when specific security and controlled events occur.
- A QAD Desktop administrative group that can access the Desktop administrative functions. This group is specified during installation of QAD Desktop 2.7 or higher.

◆ See “Administrator Group” on page 217.

Note If you plan to take advantage of the simplified screen tool in QAD Desktop 2.7, you can also specify a user group that can create and modify screen templates, which are then assigned to groups of users.

◆ See *User Guide: QAD Desktop* for details on simplified screens.

Although they can streamline security setup and administration activities, groups are not required to control access. Depending on your security requirements, you can also control access based on individual IDs or not at all.

♦ See “Specifying User Groups” on page 233.

You also can assign user IDs to existing groups by domain in User Maintenance (36.3.1). To use this method, just set up a group name and description in User Group Maintenance, and set Update Groups to Yes in the domain frame of User Maintenance.

Use the first frame to enter a name and description for the group. Then specify the domain with which you want to associate group records. The domain must be defined in Domain Maintenance (36.10.1), and the Active field must be Yes in that program.

Fig. 7.20
User Group
Maintenance
(36.3.4)

The screenshot shows the 'User Group Maintenance' window with the title bar 'All Domains (USD)'. The window is divided into several sections. The top section contains 'Group Name: Finance' and 'Description: Finance only'. The second section contains 'Domain: st92bmfg' and 'Name: qad.inc'. Below this is a table of assigned users:

User ID	User Name
hme1	Heather Entman
mat2	Matt Thompson

At the bottom, there is another section with 'User ID' and 'User Name' fields, where 'hme1' is entered in the User ID field and 'Heather Entman' is in the User Name field. The 'hme1' field is highlighted in yellow. The bottom right corner of the window has three buttons: a red 'X' (close), a left arrow, and a right arrow.

The system lists all users currently assigned to this domain/group combination. To add a user ID, navigate to the User ID field in the bottom frame and enter a user ID defined in User Maintenance. If the user is not currently assigned to the domain, User Group Maintenance automatically creates that association.

♦ See “Active” on page 229.

If you enter a deactivated user ID—one that has Active set to No in User Maintenance—the system displays a warning message. Although the user ID is considered part of the group, the user cannot log in to the system until the user ID is reactivated.

Deleting Group Records

To delete a user ID from the group, select the ID from the list and choose Delete. Confirm the delete to continue.

To delete a group, you must first delete all the domain-specific group records. Navigate to the Domain field and choose Delete. When you confirm the deletion, the system removes all references to the group from access lists associated with each domain. After deleting these records, the system prompts you to delete the group itself.

Note Deleting a group has no effect on access records set up using Field Security by Group (36.3.20). That program creates an individual access record for each group member; these records are not updated when a group is deleted. You must use Field Security Maintenance (36.3.19) to delete records individually by user ID.

See “Field Security by Group” on page 245.

User Group Example

In this example, the system administrator employs user groups and menu security to control access to three functions based on each employee’s organizational level.

Company A wants to provide three levels of access to accounts payable (AP) functions: one for clerks, one for managers, and one for the CFO.

The system administrator creates three groups in User Group Maintenance: *Clerk*, *Manager*, and *CFO*. Sara, the AP Clerk, is added to the Clerk group. Don, the AP Manager, is added to the Manager and Clerk groups. Helen, the CFO, is added to all three groups. In this setup, Helen’s group membership grants her entry to all the levels she is authorized to access.

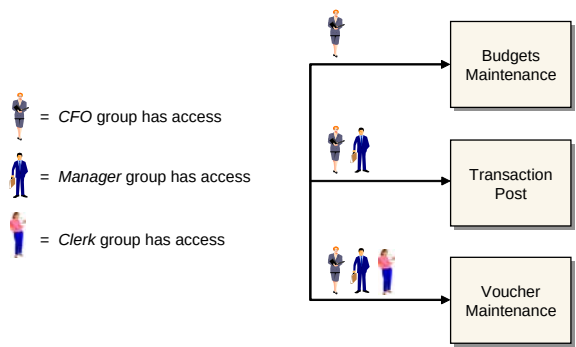


Fig. 7.21
Using Groups to
Give Access

Table 7.5 shows how the system administrator sets up user access for each group in User Group Maintenance.

Table 7.5
Sample Group
Setup

Group	User
<i>Clerk</i>	Sara
<i>Manager</i>	Don
<i>CFO</i>	Helen

Next, the administrator uses Menu Security Maintenance (36.3.10) to grant each group access to the appropriate programs.

When Mark is hired as the new deputy CFO, the system administrator only has to assign Mark to the *CFO* group—rather than using Menu Security Maintenance to give the new user access to each individual protected AP function.

Using Security Functions

You can use individual user records as well as user groups to limit system access based on the following:

Tip
Except for menu security, access records apply only to the current domain from which they are entered.

- The MFG/PRO menu system
- Individual fields
- Sites
- General ledger accounts
- Inventory movement codes

◆ See *External Interface Guide: Sales and Use Tax* for information on SUTI.

Note If you use the Sales and Use Tax Interface (SUTI) to communicate tax data between MFG/PRO and Vertex’s Quantum for Sales and Use Tax product, set up similar access controls in Tax Interface Control (36.5.3.24).

Specifying Groups or Users

To define security access by menu, site, and so on, you can enter any number of valid user IDs and/or groups, separated by commas, in the following programs:

- ◆ See page 240.
- ◆ See page 246.
- ◆ See page 249.

- Menu Security Maintenance (36.3.10)
- Site Security Maintenance (36.3.15)
- Inventory Movement Code Security (36.3.17)

- GL Account Security Maintenance (36.3.16). ♦ See page 248.
- Entity Security Maintenance (36.3.13), which is based only on user ID access. You cannot assign user groups. ♦ See page 247.

Note If you do not set up records in these programs, the system by default allows access to all users who pass log-in and domain security restrictions.

♦ See “Basic Log-In Security” on page 198.

The system validates entries against records set up in User Maintenance and User Group Maintenance.

The asterisk (*) and exclamation point (!) are special characters when used in the User IDs/Groups field.

- The asterisk (*) gives access to all users and groups.
- The exclamation point restricts specific users by user ID, not by group. For example, !user1, * means all users except user1 have access to the function; !user1, admin allows access only to members of the admin group, with the exception of user1. However, !admin, * does not prevent members of the admin group from accessing the function.
- When using the exclamation point, you must enter exclusions first: *, !user1 gives access to all users *including* user1. To exclude multiple users, enter:

!user1, !user2, !user3, *

Important When you enter exclusions, you must also define users who have access. For example, if you enter just !user1, you are specifying that user1 does not have access—but you have not granted access to other users. The result is that no one has access to the controlled function. To avoid this situation, be sure to enter the appropriate user IDs, groups, or an asterisk after the exclusions. In this example, !user1, * excludes user1, but lets all other users run the program.

- When you use the asterisk to grant access to all but specifically excluded users, the logic works correctly only when excluded users are not assigned to groups. The asterisk allows access to all group members, even if they have been excluded as individuals.

Table 7.6 lists some examples. User IDs and group names are not case-sensitive.

Table 7.6
Sample Uses of
User ID and Group
Name

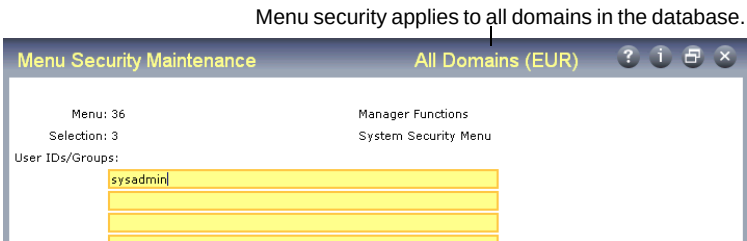
String	Description
*	All users have access.
mary, manager	Only user mary and members of the manager group have access.
!jcd, *	Everyone but user jcd has access.

The inverse of the last example does not work. If you put *, !jcd in the field, the system grants everyone access first and does not go back to check on jcd. Someone using the jcd user ID would not be excluded. In general, avoid using any exclamation point after the very beginning of the entry.

Assign Access by Menu

Menu security controls each user’s access to programs. Use Menu Security Maintenance (36.3.10) to define the users or groups that have access to a menu function.

Fig. 7.22
Menu Security
Maintenance
(36.3.10)



Specifying Menu Numbers

Enter the number identifying the menu where the program you want to restrict is found. The system combines menu and selection number to determine the function to be restricted.

For example, Purchase Order Maintenance is selection 7 on menu 5.

To restrict an entire submenu, enter the menu number in Menu and the submenu in Selection. For example, Menu 7 Selection 1 restricts the entire Sales Order Menu (7.1).

The main menu is identified by menu number 0 (zero). In the character interface, restrict access to any of the 36 top-level menu items by specifying 0 for menu and the appropriate number for selection.

In the Windows environment, top-level menu options are also grouped under seven icons. These icons are referenced through the letter A:

- A.1: Distribution
- A.2: Manufacturing
- A.3: Financials
- A.4: Customer Services
- A.5: Master Data
- A.6: Custom
- A.7: Supply Chain

To restrict access to top-level menu items in the Windows interface, define records for menu A and the appropriate selection number as well as menu 0 and the appropriate selection.

For example, to restrict access to the Item/Sites menu (1) in Windows, create the following records:

- 1 Specify Menu: 0, Selection 1.
- 2 Specify Menu A.5, Selection 1.

Important Menu security is intended to provide control over menu functions as opposed to the executable programs associated with a particular menu specification. This distinction is important in cases where a particular function is provided in multiple menu locations. For example, AR Aging as of Effective Date (arcsrp05.p) exists at the following menu locations:

- 26.21.1.12.16
- 26.21.3.1.16
- 27.18

If User1 is denied permission to execute this function from the first two menu locations, this user may still be able to execute the function from the third location.

Effect of Menu Security

The effect of menu security varies according to the interface.

- In the character interface, users cannot see restricted menu items or submenus.
- In the Windows interface, a restricted menu item or submenu displays with an X after the menu number. Users can choose not to see restricted menus by selecting Hide Menu Items from the Options menu.
- In QAD Desktop, restricted menus display but users cannot execute them.

◆ See “Progress Editor Access” on page 202.

In all interfaces, users cannot access a restricted menu item by typing the program name. However, programs can still be executed from the Progress editor unless you add security for it. To do this, leave Menu blank in Menu Security Maintenance and specify selection 1, which represents the editor.

Limit Access to Fields

Field security prevents unauthorized users from updating secured fields. It does not prevent them from seeing the value of a field if they have access to the screen where it is updated. Neither does it protect a field from program-level updates through custom code.

◆ See “Specifying Groups or Users” on page 238.

The system determines whether a user is authorized based on whether the user ID matches the values specified for the field. User groups are supported through a two-step process.

Field Security Validation

In the standard release of MFG/PRO, security is not active for any fields, and only a few fields are eligible for field security. Use the Dictionary Field Security Report (36.3.23.20) to determine which fields can be given security.

In the character and Windows interfaces, you can also access the field on a screen and press Ctrl+F. The information window indicates whether password validation is available for the field.

An eligible field must have a specific validation expression in the data dictionary. The expression must reference `gppswd.v`. The syntax is:

```
{gppswd.v &field=<dictionary field name>}
```

Activated Field Security Report

Use the Activated Field Security Report (36.3.23.19) to see which fields have security activated. It also lists privileged user IDs.

Dictionary Field Security Report

The Dictionary Field Security Report (36.3.20) lists the fields containing the association to the validation file as part of their definition.

Protect any of these fields from update by creating a record of privileged user IDs or groups. This association can be made to any field, and is one of the only database definition changes you can make that does not constitute a schema change.

Adding Security to an Eligible Field

- 1 Add the field name and the list of user IDs that can access the field in Field Security Maintenance (36.3.19).
- 2 Verify that the field is secured by running the Activated Field Security Report (36.3.23.19).

Adding Field Security Eligibility

You can make most fields eligible for field security by adding the validation expression to the field in the data dictionary. You then recompile the programs that use the field, using the modified data dictionary. It is not always possible to add field security. Some fields have preexisting data dictionary validation expressions that prevent the addition of `gppswd.v`.

Warning Once you have made a field eligible for field security, you cannot make it ineligible. You can deactivate the security by removing all user IDs for the field in Field Security Maintenance (36.3.19).

For multiple databases, make your security changes in the database against which you compile. The changes are then in effect for any other databases you run the compiled code against.

- 1 Identify and list all fields you want to add security to.
Since recompiles take time, it is more efficient to add all field security at once.
- 2 Make sure all other users are logged out.
- 3 Run Field Eligibility Maintenance (`mgfldcmt.p`, 36.25.22), which changes the validation expression and message in the data dictionary.
- 4 Set field security for each field on your list.
The `mgfldcmt.p` utility prompts for a table and field name on which to activate field security. Once you enter a valid field and table name and you press Go, you are prompted for the next entry.
- 5 Press End to exit Field Eligibility Maintenance.
- 6 Recompile either all programs or those programs impacted by the changed field security. If you have custom programs that access these fields, they also need to be recompiled.
To compile only the affected programs, make a backup copy of `utcompil.wrk` in the `qad` directory, and then delete the program names that you do not want recompiled from the file.
`utcompil.wrk` contains a complete list of all programs.
- 7 Back up recompiled code.
- 8 You can now add the field name and the list of user IDs that can access each field in Field Security Maintenance (36.3.19).
- 9 Verify that each field is secured by running the Activated Field Security Report (36.3.23.19).

Note For multi-language implementations, you must run `mgfldcmt.p` in the base language MFG/PRO instance. Then you must recompile your code for the base language and all other languages you have implemented.

Field Security by Group

You can also set up field security for a group of users.

- 1 Assign users to groups in User Group Maintenance (36.3.4) or User Maintenance (36.3.1).
- 2 Execute Field Security by Group (36.3.20). This function adds all users who belong to a specified group to the list of authorized users for a validated field.

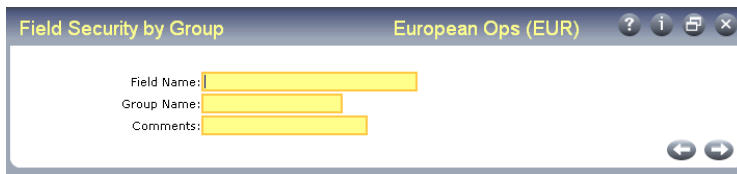


Fig. 7.23
Field Security by
Group (36.3.20)

Even with this process, field security is only available at the user level, not the group level. Field Security by Group is simply a batch utility that lets you add multiple individuals simultaneously. This has the following consequences:

- If you remove a user from a group that was given access to a field, that user can still access the field. To prevent this, use Field Security Maintenance (36.3.19) to remove the individual user.
- You cannot use Field Security by Group to remove a group of users from the list of authorized users. To remove a group, you must remove every individual in the group in Field Security Maintenance.
- If you delete a group in User Group Maintenance, individual records remain on the system until you delete them in Field Security Maintenance.

Once Field Security by Group is executed for a field and group, all users who belong to the group display in Field Security Maintenance as authorized to access the field. The Comments field in Field Security by Group displays as the comment for the field and user combination in Field Security Maintenance.

Control Inventory Access by Site

Site security lets administrators control user access to inventory transactions at each site in a domain. Only authorized users can process transactions at secured sites.

Access is managed by user and by group. A user can access a site only if that user's ID or group name appears in the Groups field in Site Security Maintenance (36.3.15).

Fig. 7.24
Site Security
Maintenance
(36.3.15)



When a user enters a restricted site code in a site-controlled program, the system checks the value of the Groups field associated with the site in Site Security Maintenance. If the user does not belong to an associated group, or the user is not given specific access by user ID, an error message displays and the user cannot complete the transaction.

Programs Affected

- Site security works with programs that change inventory data and have a Site field as part of the selection criteria.
- Site security checks ranges of sites on batch update programs that meet the previous criteria: they affect inventory and have a Site field. This includes programs such as Regenerate Materials Plan (23.2) and Sales Order Auto Allocations (7.1.17).
- Site security does not affect inquiry and report programs.
- Delete and archive programs, Contract Control (11.5.24), and Quality Management Control (19.24) do not use site security.
- You must set up each domain individually.

Implementing Site Security

Because of the complexities of MFG/PRO security, it is important to plan site security carefully and to follow closely the procedures for creating user and group names and associations. Users who are not listed individually or who have no group memberships in Site Security Maintenance (36.3.15) cannot complete transactions at secured sites.

To implement site security, associate groups with users in User Maintenance or User Group Maintenance.

♦ See “Specifying Groups or Users” on page 238.

Ranges of Sites

Many programs let you access a range of sites at one time. Site security controls data updates and processes for ranges of sites. If you enter a range of sites, you must have access to all of them for the update to occur.

When you enter a range of sites that includes sites you do not have access to, an error message displays for the first site code from which you are restricted. You must then adjust the site range to include only sites that you can access.

Control Entity Access

When entity security is in place, only authorized users can complete update transactions in the General Ledger module for particular entities. Update transactions include:

- Transaction maintenance
- Posting
- Consolidation
- Export and import
- Budget maintenance
- Opening and closing fiscal periods

Entity security also affects the following programs in other modules:

- Debit/Credit Memo Maintenance (27.1)
- Payment Maintenance (27.6.4)
- Voucher Maintenance (28.1)

- Voucher Confirmation–Automatic (28.6)
- Voucher Confirmation–Manual (28.7)
- Cash Book Maintenance (31.13)
- Fixed Asset Transaction Post (32.13)
- Fixed Asset Transaction Void (32.14)
- Fixed Asset Retirement (32.19)

All users can still enter maintenance functions or run inquiries and reports. To control access to a screen, you must use menu security.

Once you define entity security for one user and one entity, it applies to all users and entities. Each user must be set up individually. To give a user access, enter the user ID and list of entities, as shown in Figure 7.25.

Note Entity security cannot be defined for groups.

Fig. 7.25
Entity Security
Maintenance
(36.3.13)

Line	Entity	Description
1	1000	Test Company Primary

An asterisk in the Entity field indicates that a user can access all entities.

Important For a user to create a new entity, they must have access to all entities (*).

Define GL Account Security

GL account security lets you restrict who can update GL accounts based on user ID or user group. Account security is only effective when Verify GL Accounts is Yes in Domain/Account Control (36.1).

Use GL Account Security Maintenance (36.3.16) to assign users or security groups to account numbers. Use the GL Account Security Report (36.3.23.16) to list all accounts that have controlled access.

♦ See “Specifying Groups or Users” on page 238.

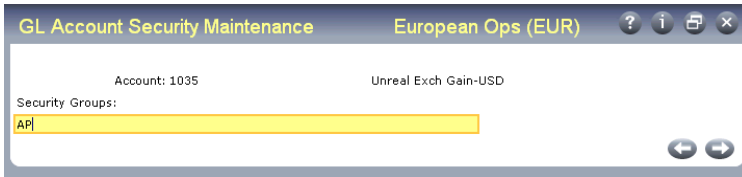


Fig. 7.26
GL Account
Security (36.3.16)

When a user attempts to create a transaction affecting an account, the system checks the user ID and the groups associated with the user against the list associated with the account. If a match is not found, a message displays and the user cannot complete the transaction.

Note Account security is not applied during Transaction Post. Use Menu Security Maintenance (36.3.10) to restrict posting functions.

Define Inventory Movement Code Security

Use Inventory Movement Code Security (36.3.17) to grant or deny access to individuals and groups to shipping transactions that reference a specific inventory movement code at a particular site.



Fig. 7.27
Inventory
Movement Code
Security (36.3.17)

When you create shippers, the system determines which inventory movement codes are available based on the Ship-From site of the shipper. Access to the inventory movement code also determines if you can select an existing shipper for maintenance.

Note Inventory movement security does not affect whether a line item from a given sales order or other originating transaction can be added to a shipper.

You can delete inventory movement security records at any time.

▶ See *User Guide*
Volume 2A:
Distribution.

Use Inventory Movement Code Security Browse (36.3.18) to display inventory movement code security records. Fields associated with a record can be viewed by scrolling the display to the left or right. Fields available as filtering parameters in Browse Options are also available on the Sort By selection list.

Monitoring System Security

Particularly in environments where security procedures are subject to regulatory controls, system administrators need methods of tracking security-related events.

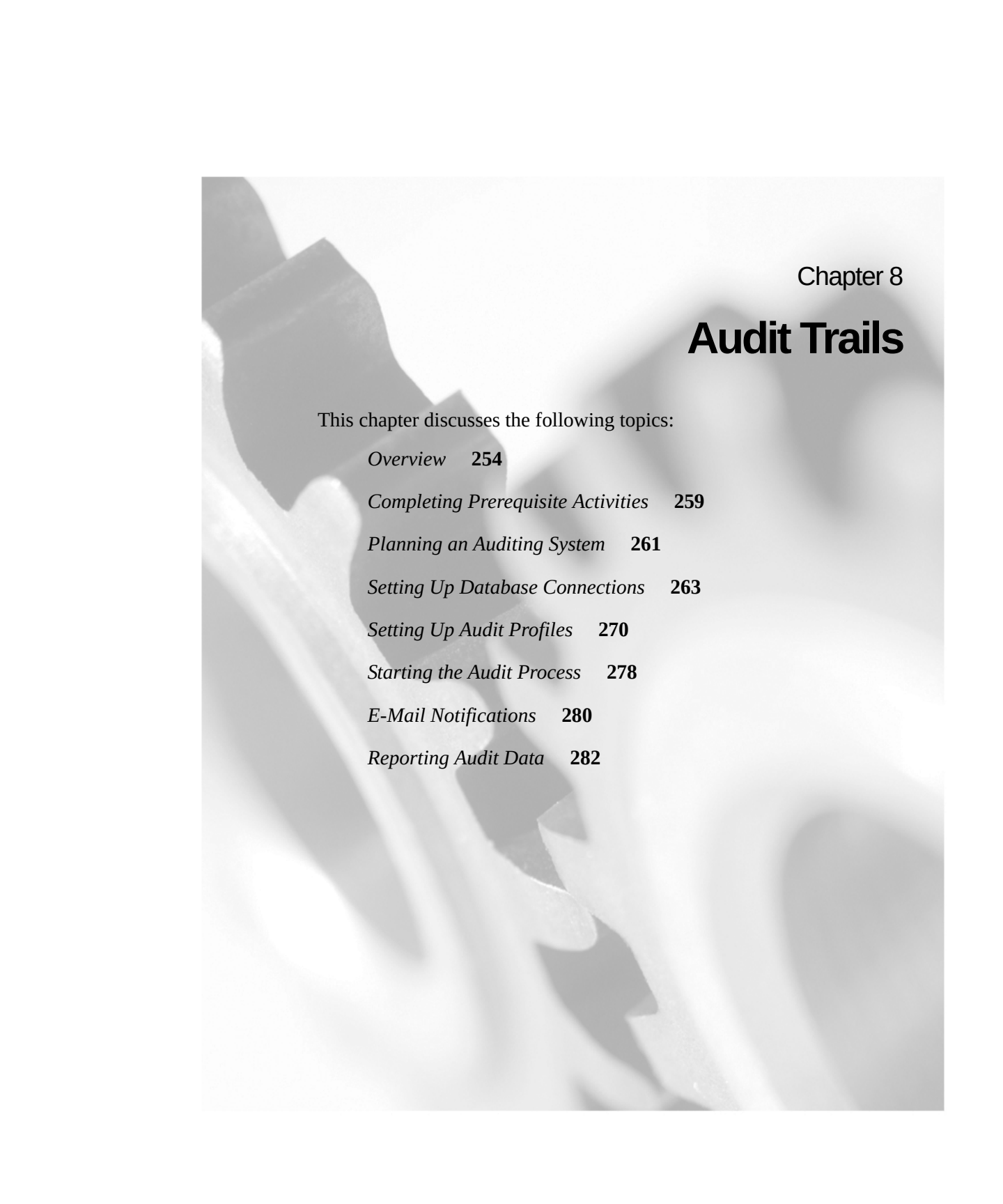
MFG/PRO provides automatic features to help administrators control and monitor security activities:

- Based on settings in Security Control, users who enter an incorrect user ID/password combination more than a specified number of times are automatically locked out of the system. They can use their user ID again only after the system administrator has reactivated it.
- When an account is deactivated, the e-mail system can automatically notify members of the administrator group. This serves two purposes:
 - In cases where the user simply forgot a password or mistyped it repeatedly, the administrator can quickly restore access.
 - The administrator knows immediately if an unauthorized user is attempting to access the system with a known user ID. This lets the administrator take appropriate steps such as immediately requiring all users to change their passwords. User Password Force Change Utility (36.3.23.12) lets the administrator force users to update their passwords based on user group, domain, and/or the date of the last change.
- Depending on the level of log-in history specified in Security Control, use Logon Attempt Report (36.3.23.1) to track when log-in attempts take place. This could be useful, for example, to track specific times when unauthorized users are attempting to access the system. The report shows such information as the user ID of the person who attempted the log-in, as well as the date, time, server time zone, and other data relevant to the log-in event.

Tip
If you are using electronic signatures, E-Signature Failure Report (36.12.7) lets you monitor unsuccessful signature events. See page 324.

Example You can set up batch processing to run this program each morning to identify all failed log-in attempts on the previous day.

- Each time a user account is activated or deactivated, the Active Reason Code field in User Maintenance must be updated. This happens automatically when an account is deactivated as a result of excess unsuccessful log-in attempts. Otherwise, the administrator must enter a reason code manually.

The background of the page features a grayscale image of several interlocking gears. The gears are of different sizes and are positioned in a way that creates a sense of depth and mechanical complexity. The lighting is soft, highlighting the teeth of the gears and creating subtle shadows.

Chapter 8

Audit Trails

This chapter discusses the following topics:

<i>Overview</i>	254
<i>Completing Prerequisite Activities</i>	259
<i>Planning an Auditing System</i>	261
<i>Setting Up Database Connections</i>	263
<i>Setting Up Audit Profiles</i>	270
<i>Starting the Audit Process</i>	278
<i>E-Mail Notifications</i>	280
<i>Reporting Audit Data</i>	282

Overview

Using this feature of the Enhanced Controls module, you can configure your system to maintain audit trails. Audit-trail records are created and stored in an MFG/PRO audit database. They contain facts about changes made in the MFG/PRO primary database. A typical audit record includes information that helps you identify who made a change, when the change was made, and what the change was. You can set up these functions for all MFG/PRO primary database tables or you can limit the audit trail recording activity to specific database tables.

Note Currently only changes to tables in the qaddb database can be tracked.

The auditing system maintains audit information based on an audit profile. An *audit profile* is a definition associated with a specific database table that indicates whether audit functionality is turned on and contains a list of the system and user-defined *delete event keys*. These key fields are used to create search criteria that enable the audit trail reports to find audit information for deleted records.

Auditing Process Work Flow

Use the programs in the Audit Trail Setup Menu (36.12.13) to set up and configure auditing functions. Figure 8.1 illustrates the auditing process work flow; use it to set up auditing functions in your environment.

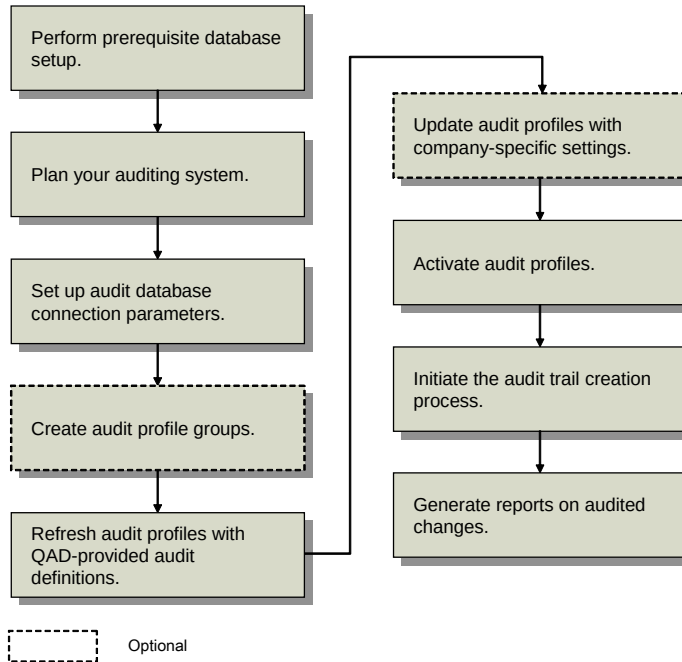


Fig. 8.1
Audit Trail
Setup Flow

Before the auditing process can begin, the prerequisite implementation and planning steps must be completed. Implementation steps include specifying the unique OID generator code for the database, adding triggers to the MFG/PRO Progress database, creating the audit schema holder in Oracle environments, setting up audit databases, and ensuring that a system administrator group has been defined to monitor auditing notifications.

◆ See page 259.

Planning steps include developing a detailed auditing plan containing a list of the MFG/PRO tables to be audited and a detailed data management strategy.

◆ See page 261.

Note The audit plan should be part of a detailed security plan to meet your business requirements. See “Security in MFG/PRO” on page 194.

Within MFG/PRO, the first activity in setting up auditing functions is to create the records that specify the audit database connection parameters and the effective dates using Audit DB Maintenance (36.12.13.11). You also indicate if each audit database is online or offline. For each connection record, you specify a parameter file or the parameters to use for connecting to the audit database.

◆ See page 263.

◆ See “Electronic Signatures and Audit Databases” on page 258.

Note Electronic signature functionality uses audit databases for archiving signature records when you use E-Signature Archive/Delete (36.12.14.22). You can use the same databases where audit trail information is stored or set up separate audit databases just for archiving signature records.

◆ See page 271.

To avoid repetitive data entry for individual table profiles, create audit groups consisting of sets of related tables to audit in Audit Group Maintenance (36.12.13.1), then refresh the table profiles in Audit Workbench Refresh (36.12.13.4) for each group. Table profiles do not exist until they are manually updated with the QAD-provided information using Audit Workbench Refresh.

An audit group is simply a group of tables. Creating an audit group removes the requirement that each table profile must be refreshed individually. When an audit group is refreshed, profiles for all member tables are automatically refreshed. This saves time and can be used to organize table profiles into functionally similar groups.

◆ See page 275.

After refreshing the table profiles, you can manually update profiles in Audit Workbench Profile Maintenance (36.12.13.5) to turn auditing functions on or off and to specify additional delete event keys. Alternatively, the default QAD-provided delete event keys are used if the profile is not updated.

◆ See page 277.

To begin auditing, activate the profiles with Audit Profile Activation (36.12.13.8). Activated profiles are staged for auditing to begin on a future date; auditing does not occur immediately after a profile is activated. On the specified begin date, the system begins generating auditing information for each table profile.

◆ See page 277.

Start the process that commits audit data to the audit database in Audit Trail Creation Process (36.12.13.23). Generated audit information is temporarily staged in an MFG/PRO database table where it is retrieved by the audit trail creation process and committed to the audit database. This approach minimizes the impact of generating audit data on system performance.

◆ See page 282.

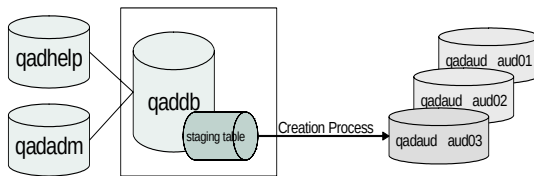
Use Audit Trail Report – Existing (36.12.1) and Audit Trail Report – Deleted (36.12.2) to report audit information. You can run reports on the audit data only after it has been committed to an audit database and only if the audit database is still online.

Audit Trail Data Flow

Audit trail functions use a separate database (qadaud) to store the audit trail data. These records are linked to records in the standard MFG/PRO database (qaddb) by the unique object ID associated with the records.

Audit data is initially saved in a staging table in qaddb. The audit trail creation process then moves audit data from the staging table and commits it to the audit database. It uses the data defined in Audit DB Maintenance to determine which database to connect to as well as the required connection parameters.

Figure 8.2 illustrates the basic flow of data.



► See “Setting Up Database Connections” on page 263.

Fig. 8.2
Audit Trail
Creation Process
Data Flow

In Figure 8.2, three audit databases are displayed. As part of implementation planning, each company must determine how frequently a new audit database needs to be brought online based on sizing requirements. The size of the audit database depends on the number of tables you decide to audit and the number of changes to records in those tables.

While only one database is updated at a time, you can generate reports for records stored in any number of audit databases.

The audit trail creation process can be started automatically by the system administrator using a custom startup script. It can also be started in MFG/PRO using Audit Trail Creation Process (36.12.13.23). If your environment generates large amounts of audit information, you can run multiple processes.

The creation process runs constantly in a dedicated MFG/PRO session, commonly referred to as a background process. It continues to commit data generated prior to 12:00 AM (midnight) until all records for a specific day have been committed to the current audit database. Once it

► See *Installation Guide: Enhanced Controls* for guidelines to consider when planning database sizing.

► See “Starting the Audit Process” on page 278.

finishes committing data for the day, the system reviews database connection records and connects to a new database if required, based on the database active date setting. It then continues recording activities for the new day.

▶ See “Audit Trail Creation Process Connection Error” on page 281.

If the creation process cannot connect to the audit database using the connection records defined for the current day, an e-mail is sent to the system administrators and a message is written in the audit log file. Audit data continues to be stored in the staging table in qaddb, ensuring that no auditable events are missed. Once the audit database becomes available, the Audit Trail Creation Process commits the saved data to it.

Important System administrators should monitor the log file to ensure the audit update process is running successfully. Certain error conditions do not generate an e-mail message; for example, a server crash.

▶ See “Audit Trail Creation Process Write Error” on page 281.

When delete event data is committed, as an additional safety measure, the system verifies the key field data. In the rare event that the validation fails, the audit data is automatically stored in a backup audit error table. An e-mail is generated notifying the administrator group of the problem. The problem data must be manually corrected by the system administrator. Contact the QAD Support organization for assistance in performing this task.

Electronic Signatures and Audit Databases

If you also use MFG/PRO’s Electronic Signatures features, you should be aware that there are relationships between that functionality and the audit databases.

▶ See “Archiving and Restoring Records” on page 329.

The electronic signature archive function does not work the same way as typical MFG/PRO archiving, which copies records from the database to operating system files. In electronic signature archiving, the system copies records to an online audit database, from which they can be restored to the system.

▶ See “Setting Up Database Connections” on page 263.

Depending on database setup, you can either:

- Use the same database that stores audit trail information.
- Create a separate audit database specifically for archived electronic signature records.

Note Regardless of which method you use, the audit databases that apply to the electronic signature records being archived or restored must be online when you run the archive or restore function.

Completing Prerequisite Activities

Before setting up the auditing features, you must complete the following prerequisite activities:

- Define an OID generator code. The system prompts for this code during installation or conversion.
- Create, configure, and start audit databases. These tasks are performed outside MFG/PRO using MFG/UTIL before any auditing information can be successfully saved to an audit database. For details, see the MFG/PRO eB2.1 *Installation Guide: Enhanced Controls*.
- Set up an administrator group in Security Control (36.3.24) to receive automatically generated e-mail notifications related to audit processing. This group also receives e-mail notifications for security violations and failed e-signature attempts.

▶ See
“Administrator
Group” on
page 217.

Note These activities, while related to auditing, are described more fully in other documentation. This section provides an overview of the activities and how they affect the auditing process. Refer to the referenced documentation for additional details.

Specify the OID Generator Code

During installation or upgrade conversion, the system prompts you to enter the OID generator code. You can choose any code that you want. However, Progress Software Corporation offers its customers the opportunity to register for unique IDs so other companies will not use the same number, maintaining uniqueness world wide.

QAD highly recommends that you obtain a code by registering each of your databases for a Dynamics Site Number from Progress Software Corporation. For details and registration, see the information at the following Progress sites:

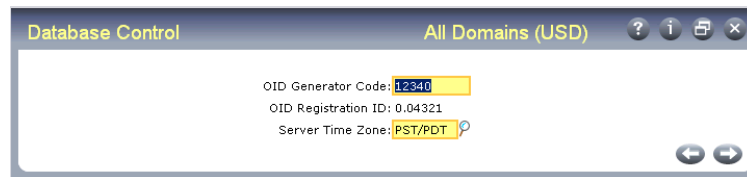
<http://www.progress.com/dynamics/sitenumbers>

http://psdn.progress.com/library/docs/site_number_faq.pdf

In a multiple-database environment, you should obtain an ID for each database. Each qaddb database is assigned its own ID so that the ID values remain unique even when records are merged into one database.

You can use Database Control (36.24) to change the generator code for a particular MFG/PRO database. Modifying the OID Generator Code does not change the OID values for existing records. After you make the change, the OID values for all new records will include the new generator code.

Fig. 8.3
Database Control
(36.24)



Based on the OID generator code, the OID fields in the database are populated using an algorithm that ensures uniqueness across all records, tables, and MFG/PRO databases within the company. The value stored in the OID field for each record has the following decimal format:

`<date><seq_value>.<registration_id>`

Where:

`<date>` is the server date with format `yyymmdd`.

`<seq_value>` is obtained from a Progress database sequence.

`<registration_id>` identifies the origin of the OID value.

The registration ID is derived from the OID generator code by reversing the digits of the generator code value and placing the decimal point in front of the result.

Create and Configure Audit Databases

Audit databases must be created outside of MFG/PRO. This guide assumes you have already created one or more audit databases. You must have an audit database configured and running before the auditing

functions can connect to it. The audit database creation and maintenance tasks are detailed in MFG/PRO eB2.1 *Installation Guide: Enhanced Controls*.

You define the parameters for connecting to the auditing database in MFG/PRO using Audit DB Maintenance. This activity is described in this chapter.

Note Electronic Signatures also uses audit databases for storing archived records. As part of the creation and configuration process, you should consider whether you want to use separate audit databases just for this purpose, or use the same database for both audit trails and electronic signature archives.

◆ See “Setting Up Database Connections” on page 263.

◆ See “Identifying the Database Type” on page 266.

Define an Administrator Group

Audit trail functions use the MFG/PRO administrator group and e-mail functions to send e-mail alerts when profiles are activated, audit information cannot be committed to an audit database, or a connection to the audit database cannot be created successfully.

◆ See “Administrator Group” on page 217.

If an administrator group is not already defined in Security Control (36.3.24), specify an existing user group as the administrator group. Alternatively, create a new user group in User Group Maintenance (36.3.21.18) and define it as the administrator group.

Each member of the group must have an associated e-mail definition specified in the user profile record created in User Maintenance (36.3.1) in order to receive e-mail notifications from the system.

◆ See “E-Mail Notifications” on page 280.

Planning an Auditing System

Every environment has unique record-keeping requirements. Before you begin setting up the auditing functions, consider creating:

- A detailed data retention plan including details such as:
 - A detailed list of the types of information you need to audit
 - A detailed list of the MFG/PRO database tables that contain information you need to audit
- A system resource and hardware plan with disk space and system resource availability

- A maintenance schedule for planning when new audit databases are created and brought online
- An information retention plan detailing how long auditing information is kept online for reporting purposes
- An archive plan detailing when audit databases are taken offline and where they are stored

Consider the following points:

- The number of database tables you maintain information for and the number of audited transactions occurring on your system are directly related to the system resource usage and availability. These factors directly affect maintenance requirements and administrative overhead.
- If you plan to use Electronic Signatures functionality, the frequency with which you will archive signature records can have a significant impact on whether you set up signature-specific databases or simply use the same databases for both audit trails and signature archives.
- The MFG/PRO information that is important to you may reside across multiple database tables. Additional research is required to find all the database tables containing this information.
- Depending on which modules you are licensed to use, some tables in the MFG/PRO database are not used and can be disregarded.
- For research purposes, you should be familiar with the Progress Database Dictionary and the MFG/PRO *Entity Diagrams* and *Database Definitions* reference guides.
- Some environments, such as in the medical industry, have very specific and stringent electronic information retention regulations; make sure you are familiar with any regulations or standards in your specific industry or region.
- For additional security, you may want to store offline audit databases on read-only media such as CD-ROMs.

Multi-Database Environments

Implementing auditing in multi-database environments has no additional special requirements. Each database in these environments has its own audit database. You set up and define audit profiles in each database, then

use different audit databases to store the audit information. Each database requires separate connection records for its specific audit databases. An audit trail creation process runs in each database, committing audit information to the appropriate audit database.

Figure 8.4 shows a typical multi-database environment layout. Notice that each database has its own unique audit staging table and audit databases.

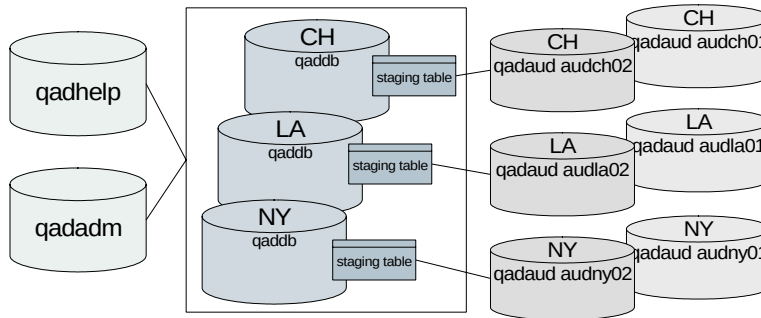


Fig. 8.4
Multi-Database
Environment
Layout

Setting Up Database Connections

Use Audit DB Maintenance (36.12.13.11) to create and maintain connection parameters and active date range information for the system audit databases. These connection parameters are used by these functions:

- The Audit Trail Report – Existing and Audit Trail Report – Deleted use the connection records to connect to the proper audit databases when reporting audit information.
- The Audit Trail Creation Process uses the connection record information to connect to the current active audit database when it needs to commit audit information from the staging area.
- If you use the Electronic Signatures function, the system uses the records to connect to the appropriate databases during signature archive and restore activities.

► See “Archiving and Restoring Records” on page 329.

This program is similar to Database Connection Maintenance (36.6.1), but has some important differences:

- You do not specify a logical name for the connection. The logical name is managed internally by the system.

- You must specify a type of ORACLE if you are connecting to an Oracle database through a Progress schema holder.
- Connections to the audit databases are not permanent. The audit reports and Audit Trail Creation Process—as well as electronic signature archive and restore functions—use the connection information to connect to the audit databases as needed. These processes do not maintain a connection to an audit database after they have retrieved or committed the information they are handling.
- The system can connect to multiple audit databases simultaneously.

Important Audit databases must be configured and running before connecting to them using the connection parameters. Audit DB Maintenance does not start or stop audit databases. It only stores the connection parameters used to connect to them. You must set up external procedures to start up and shut down audit databases as needed.

► For details, see
*Installation
Guide: Enhanced
Controls.*

Example When bringing up the MFG/PRO system after a scheduled shutdown, a script is executed from the operating system. The script can be created from MFG/UTIL. Using a predefined list, the script starts up the audit databases for reporting. When the audit reports are run, they use the connection record parameters to connect to the appropriate databases and report audit information as required by the report selection criteria.

Database connection parameters are defined by the way audit databases are implemented. The system administrator that creates and maintains the MFG/PRO database provides the connection information required to set up the field values on this screen.

Fig. 8.5
Audit DB
Maintenance
(36.12.13.11)

The screenshot shows a window titled "Audit DB Maintenance" with a subtitle "All Domains (USD)". Inside the window, the "Audit Database Name" is "auditdb1" and the "Description" is "ACTIVE AUDIT DB". Below this, the "Connection Parameters" section lists the following fields:

- Database Online: ☒
- Physical Database Name: auditdb1
- Database Directory: /qad/mfgpro/91db/mdgdb/pubdb
- Host: ohhp40
- Server: pr91ny2h-server
- Type: Progress
- Network: TCP
- Parameter File: atc.pf

Navigation arrows are visible at the bottom right of the form area.

In the first frame, enter a name for this audit database connection record. The name must be 8 or less characters. It is used for tracking and maintaining your database connection information. It does not necessarily have to be the physical name given to the audit database.

Specifying Database Connection Parameters

For Progress databases, you can specify connection parameters directly in Audit DB Maintenance or include them in a parameter file. If you use a parameter file, you must still specify the database name in the Audit DB Maintenance screen. If the database is not located in the PROPATH, you must also specify the full path in Database Directory.

▶ See “Using a Parameter File” on page 267.

Note Typically, each implementation has additional parameters that are needed to accommodate specific requirements that cannot be specified directly in the maintenance screen. These can be supplied in the parameter file.

For Oracle databases, you specify some values in Audit DB Maintenance, but a parameter file is always required. This is because two sets of connections are required for Oracle databases: one for the Progress schema holder and one for the Oracle database. The values that you specify in the Audit DB Maintenance fields apply to the Progress schema holder only. Connection to the Oracle database is defined in the parameter file.

Database Online. This field indicates whether the system should attempt to connect to the audit database. It does not indicate that an audit database is running, nor that a connection to the database has been tested or is currently active.

Physical Database Name. Enter the actual physical name of the Progress database or schema holder. Database names are typically case sensitive and can be up to 12 characters long.

The database directory and physical name together make up the complete path name to this database. These are used on the database connect statement when connecting to this database.

For example, on a UNIX system if your database is stored as `/qad/d7/qadaud01.db`, then the directory is set to `/qad/d7` and the physical name is `qadaud01`. You do not need the `.db` extension.

Database Directory. Enter the complete path name of the operating system directory where this database is stored. Path names may be case sensitive and can be up to 50 characters long.

▶ See “Using a Parameter File” on page 267.

The following fields should only be specified if they are not included in a parameter file. If you do specify them with a parameter file, any values in the parameter file are used instead of these values.

Host. Enter the name of the host server where the Progress database or schema holder can be found. This name follows the -H parameter on the Progress connect statement. It is only required when the database is located on a different computer.

Server. Enter the name of the service to be used by the broker process when starting up the remote database. This name follows the -S parameter in the Progress connect statement. It is only required when the database is not located on the current machine.

Type. Specify the audit database type, either Progress or Oracle. You must use a parameter file to connect to Oracle audit databases.

Network. Enter the type of network being used. Valid values are TCP (default) and SNA (Progress/400). If left blank, TCP is assumed. This value follows the -N parameter on the Progress connect statement.

Identifying the Database Type

The audit database can serve two functions:

- Store audit trail records
- Store archived electronic signature records

Depending on the values you enter in the Database Type frame, an audit database can serve either or both of these purposes.

Fig. 8.6
Audit DB
Maintenance,
Database Type
Frame

Database Type		
Audit Trail: ☒	Begin Date: 01/01/2003	End Date:
E-Signature: ☒	Begin Date: 01/01/2004	End Date:

Cannot be updated once database contains data of the specified type.

Audit Trail, E-Signature. If you use both Audit Trails and Electronic Signatures functions, use these fields to control whether audit trail data and archived signature records are stored in separate databases. When both fields are Yes, the system uses this database for both data types. Otherwise, you can choose to set up and administer a separate database for each function.

Begin Date. Enter the date when the system should begin saving the specified type of information to the audit database identified by this connection record. Connection records become effective at 12:00 AM on the indicated date.

Setting Database Online to Yes does not start an audit database; it simply indicates that the system is allowed to save or retrieve information for the audit database. This assumes that the database has already been configured and started outside of MFG/PRO. The Begin Date must correspond to a date when the indicated database is already online; otherwise, the system reports connection errors. New audit trail creation processes cannot be launched if the system cannot connect to the current audit database. This is also true of electronic signature archive and restore activities.

End Date. This value cannot be updated manually. It is automatically updated when the system begins storing information of the specified type in a new audit database.

Note You cannot change a data type or begin date field once the system has used this database to store any data of the associated type.

Using a Parameter File

Depending on your environment, your parameter files may differ from these general guidelines.

The following guidelines apply to parameter files used to connect to a Progress database or Progress schema holder for an Oracle database:

- Specify the parameter file name in Parameter File.
- Specify connection parameters in the parameter file or in the corresponding fields. Do not include the parameters in both the file and in the corresponding fields.

- The parameter file must be accessible through the PROPATH or located in the directory specified in Database Directory.
- If you use a parameter file, you must still specify the database name in the Audit DB Maintenance screen. If the database is not located in the PROPATH, you must also specify the full path in Database Directory.
- The parameter file should not include either the `-ld` or `-db` parameters.
- The parameter file must include the `-trig` parameter that specifies the location of trigger files.

For Oracle audit databases, you specify the schema holder name in Physical Database Name and set Type to Oracle. The parameter file must include the parameters for the schema holder followed by parameters for connecting to the Oracle database, in this order:

- `-trig` parameter
- Other connection parameters for the schema holder
- `-db` parameter for the Oracle database
- The Oracle database connection parameters, including the `-dt` ORACLE parameter and the `-ld` parameter, if needed

Table 8.1 shows several sample database connection settings and corresponding parameter files.

Database Type	Audit DB Maintenance Settings	Parameter File Values
Progress	Physical Database Name: auditdb1 Database Directory: /qad/mfgpro/db Host: mainserver Server: audit1-service Type: Progress Network: TCP Parameter File: example1.pf	-trig "triggers"
Progress	Physical Database Name: auditdb1 Database Directory: /qad/mfgpro/db Host: Server: Type: Progress Network: TCP Parameter File: example2.pf	-trig "triggers" -H mainserver -S audit1-service
Oracle	Physical Database Name: audit Database Directory: /qad/mfgpro/db Host: mainserver Server: otest3-service Type: ORACLE Network: TCP Parameter File: example3.pf	-trig "triggers" -znotrim -db otest3 -dt ORACLE -U qad@otest3 -P QAD
Oracle	Physical Database Name: audit Database Directory: /qad/mfgpro/db Host: Server: Type: Network: TCP Parameter File: example4.pf	-trig "triggers" -znotrim -H mainserver -S audit1sh-service -db otest3 -dt ORACLE -U qad@otest3 -P QAD

Table 8.1
Sample Parameter
Files and Audit DB
Maintenance
Settings

Setting Up Audit Profiles

Setting up and using audit profiles include these steps:

- Create audit groups
- Refresh audit profiles
- Update audit profiles
- Activate profiles

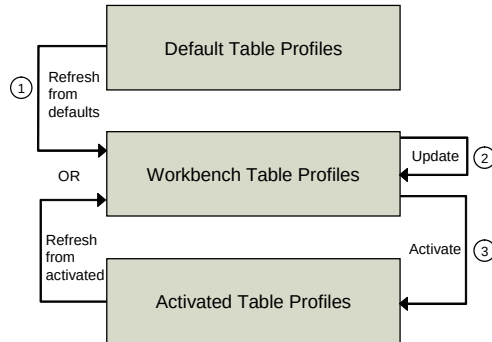
Overview

Each MFG/PRO database table has its own profile. Initially all table profiles are empty; they must be refreshed with the QAD-provided default information. Table profiles hold values that auditing functions use to manage the audit trail generation and reporting process. This information affects auditing only after the profile is activated.

A table profile:

- Indicates whether auditing is enabled
- Maintains a list of QAD-defined delete event keys
- Maintains a list of user-defined delete event keys

In addition to the QAD-provided default data, the system maintains two sets of profiles: the profiles you edit in the workbench and the activated profiles. When you activate a profile, the system creates a new activated profile by copying your completed workbench profile and setting the begin date. Since the system activates a copy of your workbench profile, you can continue to modify the workbench profile with Audit Workbench Profile Maintenance without affecting the active system.

Fig. 8.7
Table Profiles

Before refreshing workbench profiles, you can optionally create audit groups to manage several profiles more easily and streamline the data setup process. Once refreshed, modify the profiles with your requirements. You can enable or disable auditing and add delete event keys as needed. When your profiles are complete, activate them and set a begin date. To discontinue auditing a table, simply update the workbench profile to set Audit Trail to No; then activate it with the begin date set to the date auditing should stop.

Creating Audit Groups

Use Audit Group Maintenance (36.12.13.1) to group all the tables you plan to audit, or to group related database tables for auditing purposes. Audit groups streamline the setup process by letting you refresh and activate the profiles for all the member tables at once, instead of maintaining one table profile at a time.

For example, set up a financial audit group to track financial transactions and a manufacturing group to separately maintain the profiles for manufacturing transactions. Add tables to each group to accommodate your specific data tracking and maintenance requirements.

Fig. 8.8
Audit Group
Maintenance
(36.12.13.1)

Audit Group Maintenance All Domains (USD)

Group Name: Finance
Description: Financial tables for aud

Table Name	Table Label	Table Detail
abd_det	Asset Book Detail	
glcd_det	General Ledger Calendar Detail	
glc_cal	General Ledger Calendar	

Table Maintenance

Table Name:
Table Label: General Ledger Calendar

Specify a group name, up to 8 characters. An audit group cannot have the same name as a database table. Then provide a brief description and press Go to display the Table Maintenance frame. In this frame, add as many tables to the group as required. After they have been added, the tables display in the Table Detail frame.

Use Audit Group Report (36.12.13.2) to display the records defined in this program.

Refreshing Profiles

When initially setting up auditing functions, workbench table profiles are empty, and must be manually populated. Use Audit Workbench Refresh (36.12.13.4) to update the empty profiles with the QAD-provided default information. You can refresh one table at a time or optionally, refresh the profiles for an entire group of tables.

You can use this program later to restore the QAD-provided default data, modified in Audit Workbench Profile Maintenance, or to update workbench profiles based on existing activated profiles.

Note Any changes you make with this program do not affect activated profiles currently in use.

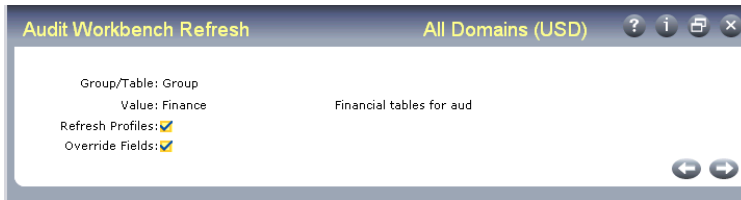


Fig. 8.9
Audit Workbench
Refresh
(36.12.13.4)

Indicate if you want to refresh tables or groups; then specify the table name or group name to be refreshed. Leave the Value field blank to refresh all tables or groups, based on the setting in the Group/Table field.

Use the following field descriptions to enter the values for the refresh process.

Refresh Profiles. Indicate whether to refresh all data for the specified profiles.

No: The Refresh Profiles frame does not display.

Yes: The Refresh Profiles frame displays. Use it to specify the source profiles for the refresh. You can use active profiles or the QAD-provided default profiles.

Override Fields. Indicate whether to override the field that controls auditing for the specified profiles. The QAD-provided default profiles have auditing functions turned on.

No: The Override Fields frame does not display.

Yes: The Override Fields frame displays for you to set the value for Audit Trail to Yes or No for all the specified profiles. If Refresh Profiles is Yes, the value specified here replaces the refreshed value.

Refresh Profile Frame

If Refresh Profiles is Yes, the Refresh Profile frame displays.

Fig. 8.10
Audit Workbench
Refresh, Refresh
Profile Frame

Source Profile. Enter Active or Default to indicate which profiles to use as the source for refreshing the profiles selected previously.

Active: Each specified workbench profile is refreshed using the activated profiles in use on the date specified in Effective On. The corresponding table profiles must be in use on the date specified; otherwise, the system displays an error for each activated profile not found and the refresh does not occur for that profile.

Default: Each specified workbench profile is refreshed using the QAD-provided values. Select this value when initially setting up audit functions to load the QAD-provided values into the profiles for the tables you plan to audit.

Tip
This field is
available only when
Source Profile is
Active.

Effective On. Enter a date when the activated source profile was in use. The workbench profile is refreshed using the active source profile settings in use on this effective date. If an activated profile was not in use on the date, an error displays and the target profile is not refreshed.

Example Enter today's date to refresh the workbench profiles based on the activated profiles currently being used.

Override Fields Frame

If Override Fields is Yes, the Override Fields frame displays.



Fig. 8.11
Audit Workbench
Refresh, Override
Fields Frame

Audit Trail. Indicate whether to enable auditing for the tables being refreshed.

If Refresh Profiles is No, the value specified here replaces the Audit Trail value in the current workbench profiles for the specified group or table.

When you refresh based on QAD-provided profiles, audit trail functions are turned on by default. You can use this field to override that setting.

Use Audit Workbench Profile Maintenance to change this value for individual table profiles.

Updating Audit Profiles

Use Audit Workbench Profile Maintenance (36.12.13.5) to adjust profile settings for your specific environment. You can enable or disable auditing and add user-defined delete event keys for the tables you plan to audit.

To disable auditing for a table already being audited, you must create a new activated profile for that table. Do this by updating the workbench profile with Audit Trail set to No; then activate that profile with the proper begin date.

Delete Event Keys

The primary index fields for each database table are defined as delete event keys. These keys are stored in the audit database when a record in this table is deleted from MFG/PRO. This is in addition to the standard information stored for create and modify auditing events. The system uses this data to uniquely identify a deleted record. This search criteria is used by Audit Trail Report – Deleted to find and retrieve deleted record information from audit databases.

Example To search for and report audit trail information for a deleted sales order, Audit Trail Report – Deleted uses a date range and the so_nbr field values indexed when the record was originally deleted. The so_nbr field is the QAD-defined delete event key for the so_mstr table.

Updating Profiles

Figure 8.12 illustrates the first frame of Audit Workbench Profile Maintenance.

Fig. 8.12
Audit Workbench
Profile Maint
(36.12.13.5)

Enter a table name and press Go. Then indicate if you want audit trail to be enabled or not. Press Go to display the delete event keys currently defined for the table.

Fig. 8.13
Audit Workbench
Profile Maint,
Delete event Key
Detail

Field Name	Field Label	Type
so_domain	_so_domain	Primary
so_nbr	Sales Order	Primary

In addition to the QAD-defined delete event keys, you can manually define any other field in the table as a delete event key in the Delete Event Key Maintenance frame.

Note You cannot delete the QAD-provided keys.

Use Audit Workbench Profile Report (36.12.13.6) to display the information updated in this program.

Activating Audit Profiles

After completing the workbench table profiles, use Audit Profile Activation (36.12.13.8) to activate profiles for one table or a group of tables. Activated profiles are staged for auditing to begin on a future date; auditing does not occur immediately after a profile is activated. On the specified begin date, the system begins generating auditing information as defined by each activated table profile.

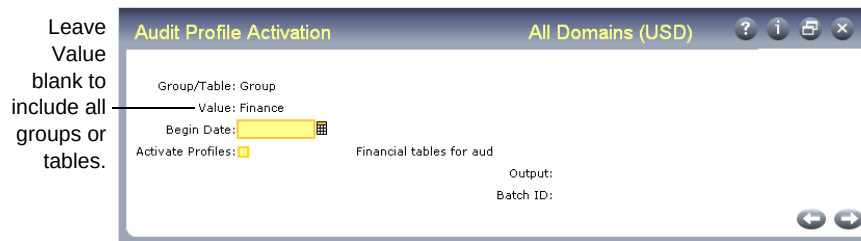


Fig. 8.14
Audit Profile
Activation
(36.12.13.8)

Profiles cannot be activated on the begin date. Plan all changes ahead of time and activate updated profiles before their begin date. Profiles must have the begin date set to sometime in the future. Activated profiles become effective at 12:00 AM on the begin date.

You can execute this program in batch mode if you are activating a group with many associated tables.

When this program completes execution, it generates a report that displays information for each table in the activated profile that includes:

- The table name and description
- Information from the active profile being replaced, if one existed, including the previous setting for begin date, audit trail, and the delete event keys

- Information from the now active profile, including the new setting for begin date, audit trail, and the delete event keys

If Activate Profiles is set to No, only the report is generated; the profiles currently in use are not updated.

See “Audit Profile Activation E-Mail” on page 280.

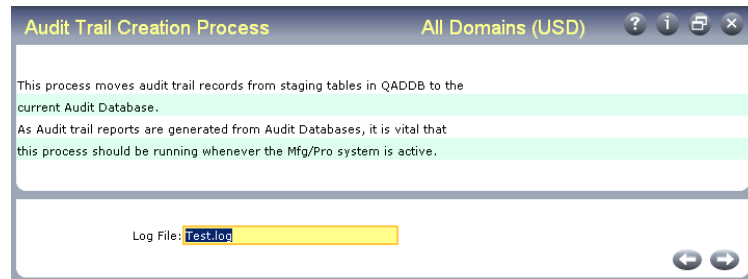
When Activate Profiles is Yes and all processing is complete, an e-mail is sent to the system administrator group defined in Security Control notifying them of the changes to the activated audit profiles.

Use Activated Audit Profile Report (36.12.13.9) to display details about activated profiles.

Starting the Audit Process

Use Audit Trail Creation Process (36.12.13.23) to start a background process that moves staged audit data from the staging table in qadddb to the appropriate audit database.

Fig. 8.15
Audit Trail
Creation Process
(36.12.13.23)



To commit generated audit information to the audit database, the Audit Trail Creation Process should be running when any active audit profiles are scheduled to become effective.

Consider using a CIM startup script to start this process automatically after system backups or downtime. Otherwise, it must be manually started whenever the MFG/PRO system is restarted.

Note *Installation Guide: Enhanced Controls* includes a sample CIM file and startup scripts for executing this program.

Audit Trail Creation Process generates e-mail messages to the system administrator group when connection errors occur. The system also saves time-stamped messages related to database connection to the log file specified in this program. These messages record when an audit process starts and ends, as well as any connection errors. Messages look like the following samples:

```
2003-12-05 @ 14:26:53 AT Creation Process session begin
2003-12-05 @ 14:27:43 Database connection failed 12-04-03
2003-12-05 @ 14:27:43 AT Creation Process session end
2003-12-05 @ 14:28:11 AT Creation Process session begin
2003-12-05 @ 14:28:11 This process was shutdown from User Account Ctrl
2003-12-05 @ 14:28:11 AT Creation Process session end
```

The log file name defaults from the value specified in User Accountability Control (36.12.13.24). You can specify a full path and file name for the log file; if only the file name is specified, the file is located in the directory where the MFG/PRO session running the audit trail creation process was started.

If multiple processes are being used, you can specify a different log file for each. If you do not specify separate log files and multiple sessions are started from the same directory, messages from each process are saved to the same log file.

♦ See “Audit Trail Creation Process Connection Error” on page 281.



Fig. 8.16
Audit Trail Control
(36.12.13.24)

To start up the creation process, the AT Creation Process Shutdown Request field must be No in Audit Trail Control.

Shut down the Audit Trail Creation Process by exiting the MFG/PRO session from where it was started. Alternatively, use Audit Trail Control to shut down all Audit Trail Creation Processes by setting the shutdown field to Yes.

E-Mail Notifications

The system generates and sends e-mails to the administrator group set up in Security Control (36.3.24) in the following situations:

- One or more audit profiles are activated.
- Errors occur when Audit Trail Creation Process writes to the audit database.
- Errors occur when Audit Trail Creation Process connects to the audit database.

The e-mail text is defined in master comment data. You can customize this text for your environment by modifying the text using Master Comment Maintenance (25.12).

The auditing messages all have a comment type of AT. The comment reference varies depending on the specific purpose. The e-mail is constructed by starting with a specific comment, followed by one or more MFG/PRO messages with additional details. A generic comment with a reference of `email_postfix` is appended. This comment contains the following information that applies to all system-generated auditing e-mails:

This email was automatically generated from an MFG/PRO process. If you have any questions about this E-mail, contact the MFG/PRO system administrator. Do not reply to this E-mail.

Audit Profile Activation E-Mail

Comment Reference: `email_profile_activation`

Comment Type: AT

The e-mail sent for audit profile activation is similar to this example.

The purpose of this E-mail is to inform you that one or more audit trail workbench profiles has been activated. You have been included in this E-mail distribution because you belong to the Administrator group identified in User Security Control for MFG/PRO. The information listed below regarding the activation can be used to obtain a detailed report of the activation by running the Audit Activated Profile Report.

The activation was performed by User ID:

The newly activated profiles are set to begin on date: dd/mm/yy

The number of newly activated profiles with the audit trail

enabled:

The number of newly activated profiles with the audit trail disabled:

This email was automatically generated from an MFG/PRO process. If you have any questions about this E-mail, contact the MFG/PRO system administrator. Do not reply to this E-mail.

Audit Trail Creation Process Write Error

Comment Reference: email_audit_creation

Comment Type: AT

The e-mail sent when the Audit Trail Creation Process detects an error while writing to the audit database is similar to this example.

The purpose of this E-mail is to inform you that one or more processing errors occurred during Audit Creation Process. You have been included in this E-mail distribution because you belong to the Administrator group identified in User Security Control for MFG/PRO.

Total Number of Processing Errors: #

This email was automatically generated from an MFG/PRO process. If you have any questions about this email, contact the MFG/PRO system administrator. Do not reply to this email.

When delete event data is committed, as an additional safety measure, the system verifies the key field data. In the rare event that the validation fails, the audit data is automatically stored in a backup audit error table. An e-mail is generated notifying the administrator group of the problem. The problem data must be manually corrected by the system administrator. Contact the QAD Support organization for assistance in performing this task.

Audit Trail Creation Process Connection Error

Comment Reference: email_creation_prefix

Comment Type: AT

The e-mail sent when Audit Trail Creation Process detects an error while connecting to the audit database is similar to this example.

The purpose of this E-mail is to inform you that the Audit Trail Creation Process was terminated. This termination is an abnormal event and should be regarded seriously. You have been included in

this E-mail distribution because you belong to the Administrator group identified in User Security Control for MFG/PRO.

<Specific connection error>

This email was automatically generated from an MFG/PRO process. If you have any questions about this email, contact the MFG/PRO system administrator. Do not reply to this email.

Three specific error messages can display in the e-mail:

- Audit database is not online. This error displays when the Database Online field is set to No in Audit DB Maintenance.
- Database connection failed. This error displays when the Database Online field is Yes for the audit database in Audit DB Maintenance (36.12.13.11), but the connect statement failed.
- Parameter file not found. This error displays when the parameter file specified for the database in Audit DB Maintenance cannot be found.

◆ See “Database Online” on page 265.

◆ See “Using a Parameter File” on page 267.

Reporting Audit Data

Use Audit Trail Report – Existing (36.12.1) and Audit Trail Report – Deleted (36.12.2) to review the historical audit trail information maintained in the online audit databases. Both reports function similarly, but one displays audit information for existing MFG/PRO records, while the other displays auditing information for deleted records.

◆ See “Setting Up Database Connections” on page 263.

These reports use the connection records maintained in Audit DB Maintenance to connect to the audit databases. They connect only during the report generation process; connections to the audit databases are not permanent.

Important Audit databases must be configured and running before running either report. The report programs do not start or stop audit databases. You must set up external procedures to start and shut down audit databases as needed. If the databases required by the report dates are not available, error messages are generated.

Displaying Existing Audit Data

Use Audit Trail Report – Existing (36.12.1) to find audit information related to existing MFG/PRO database records. You can only report against audit databases that are currently online.

Note This report does not display audit information for deleted MFG/PRO records. To see audit information for deleted records, use Audit Trail Report – Deleted.

See “Displaying Deleted Audit Data” on page 285.

Figure 8.17 illustrates the first frame of Audit Trail Report – Existing.

Fig. 8.17
Audit Trail
Report – Existing
(36.12.1)

Select the table, user ID, date range, and report style in the first selection criteria frame. You also indicate if you want all the fields in the selected tables to be included in the report by default. You can modify the setting for individual fields as needed in the Report Display Fields frame.

Then press Go to display the E-Record Selection Criteria frame where you can specify a range of values for one or more fields for identifying the MFG/PRO records to report.

T	Field Label - Name	From Value	To Value
P	Domain - so_domain	st92bmfg	st92bmfg
P	Sales Order - so_nbr		
I	Bill-To - so_bill		
I	Call - so_ca_nbr		
I	End Customer PO - so_cust_po		
I	FSM Type - so_fsm_type		
I	Invoice Number - so_inv_nbr		
I	oid_so_mstr - oid_so_mstr		

Fig. 8.18
E-Signature History
Report, E-Record
Selection Criteria

This frame displays the field name, field label, and field type for each field in the selected database table. Field types are Primary (P), Indexed (I), or non-indexed (F). To enter a selection range for a field, navigate to the Data Range frame, where you can specify from and to values. Any selection criteria entered in the Data Range frame display next to the corresponding field on the E-Record Selection Criteria frame. These selection criteria are used to narrow the search results. Not entering a data range for a field matches all values.

Note Large reports may result if you do not specify field-level selection criteria.

To minimize the report output, enter criteria for as many table fields as needed. For example, if you are reporting the audit trails for one or more so_mstr records, scroll to the so_nbr field and press Go. Enter a range of sales order numbers in the so_nbr From Value and To Value fields to narrow the search results. After entering the field-specific selection criteria for your report, press End to continue.

Use the Report Display Fields frame to select or deselect the fields to include or exclude on the resulting report.

Fig. 8.19
Audit Trail
Report – Existing,
Report Display
Fields

Sel		T	Field Label	Field Name
*	F		Accrued Revenue	so_fsacorr_acct
*	F		Accrued Revenue Sub-Acct	so_fsacorr_sub
*	F		Accrued Revenue CC	so_fsacorr_cc
*	F		Action Status	so_stat
*	F		AR Account	so_ar_acct
*	F		AR Sub-Account	so_ar_sub
*	F		AUTHNBR Unique Days	so_auth_days
*	F		Auto Replenish	so_auto_replenish
*	F		Bank	so_bank
*	F		BOL	so_bol
*	F		Cancel Date	so_cncl_date
*	F		Cartons	so_cartons
*	F		Channel	so_channel

All fields are preselected if Auto-Select All is Yes in the first frame. Select or deselect fields as needed. Then press Go to specify the output device for the report.

Displaying Deleted Audit Data

Audit Trail Report – Deleted (36.12.2) shows a complete history for any audited MFG/PRO record that has been deleted. The report includes two date ranges. The first date range indicates the range of audit trail event dates to include in the report. The second date range, Delete Date and To, refers to the date the record was actually deleted.

The date range is not mandatory, but entering one narrows the search of audit databases and improves reporting speed. If older audit databases have been taken off-line, restrict the date range to dates included in the online databases to avoid error messages.

Example Several records were deleted sometime in June 2004. You need to see the previous year's audit trail information for those records. Enter 07/1/03 to 06/30/04 in the first date range to see events that occurred in the previous year. In the second date range, enter the date range when you think the records were deleted, 06/01/04 to 06/30/04.

The resulting report shows that the last audit event for the reported records was DELETE with an event date of 06/02/04. The report also shows the CREATE and MODIFY events for the records if these events occurred in the previous year.

Figure 8.17 illustrates the first frame of Audit Trail Report – Deleted.

The screenshot shows a software window titled "Audit Trail Report - Deleted" with a subtitle "All Domains (USD)". Inside the window, there are several input fields: "Table Name:", "User ID:", "Date:", and "To:". The "Date:" field is highlighted with a yellow box and has a label "Date range for audited events" pointing to it. Below these fields are "Summary/Detail: Summary" and "Auto-Select All:". There are also navigation buttons at the bottom right.

Fig. 8.20
Audit Trail
Report – Deleted
(36.12.2)

This frame is the same as Audit Trail Report – Existing. Select the table, user ID, date range, report style, and selection default. When you press Go, you are prompted for a date range when the deletions occurred. If you do not know this, enter a date range spanning the online audit databases.

Fig. 8.21
Audit Trail
Report – Deleted,
Date Range

The screenshot shows a window titled "Audit Trail Report - Deleted" with a subtitle "All Domains (USD)". It contains two input fields: "Delete Date:" and "To:". A label "Date range for deletion" with an arrow points to the "Delete Date:" field. The window also displays "Table Name: so_mstr" and "Sales Order Master".

Enter an appropriate date range and press Go. The Deleted E-Record Selection Criteria frame displays.

Fig. 8.22
Audit Trail
Report – Deleted,
Deleted E-Record
Selection Criteria

The screenshot shows the same window as Fig. 8.21, but with the "Deleted E-Record Selection Criteria" frame displayed. This frame contains a table with the following data:

T	Field Label - Name	Value
P	Domain - so_domain	st92bmfg
P	Sales Order - so_nbr	
I	oid_so_mstr - oid_so_mstr	

Below the table, there is a "Field Name:" field with "so_nbr" entered and a "Data Value" field with a question mark. The window also displays "Table Name: so_mstr" and "Sales Order Master".

The field name, field label, type, and value for the associated delete event keys display in the Deleted E-Record Selection Criteria frame. Field types are Primary (P), Indexed (I), or non-indexed (F). To identify the deleted MFG/PRO record, you can enter specific search criteria for each delete event key or choose Go to continue. To enter specific data values for an event key, select the key and then enter the criteria in the Value field. Press End when you finish entering values. The Report Display Fields frame displays.

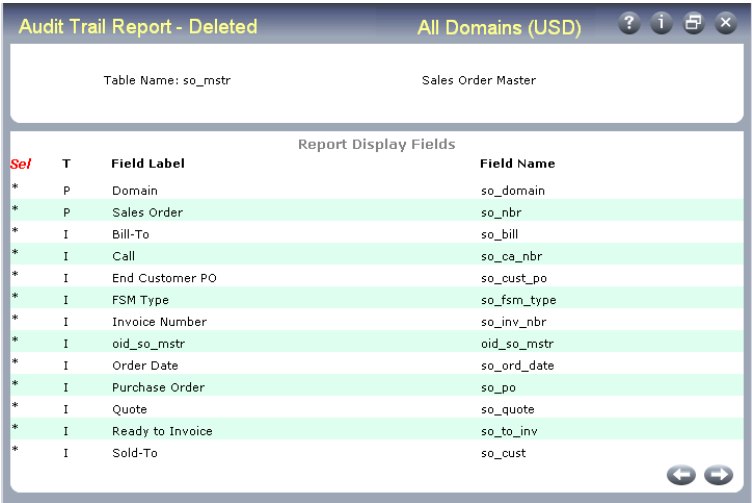


Fig. 8.23
Audit Trail
Report – Deleted,
Report Display
Fields

This is identical to the frame that displays in Audit Trail Report – Existing. It displays all the fields in the table for which you are generating a report. All fields are preselected if Auto-Select All is Yes. Select or deselect fields as needed. Then press Go to specify the output device for the report.

Electronic Signatures

This chapter discusses the following topics:

Overview **290**

Completing Prerequisite Activities **301**

Defining Electronic Signature Profiles **303**

Recording Electronic Signatures **316**

E-Mail Notifications **321**

Reporting **322**

Archiving and Restoring Records **329**

Overview

Particularly in areas with critical processes that rely on tight quality control such as the pharmaceuticals industry, regulatory guidance often requires records to be signed by an author, approver, tester, or other accountable individual.

While this signature process is historically associated with a hard-copy signature on paper, it has been extended in many areas to electronic records. For example, the United States Food and Drug Administration (FDA), in 21 CFR Part 11, describes how electronic signatures can be used to support automated processing.

The electronic signatures features of the Enhanced Controls module support this requirement. You can configure your system to require users of some MFG/PRO programs to enter a valid user ID and password before they can create or update records. Additionally, they must provide a reason code that defines the meaning of the signature; for example, Approved or Tested. Based on setup data, users may be able to enter a related remark as part of the signature.

◆ See “Assign Access by Menu” on page 240.

Note Any valid user who has access to a program that records signatures can sign records. Use Menu Security (36.3.10) to assign access to signature-controlled functions based on user groups or individual user IDs.

These features are intended as part of an overall approach—also incorporating capabilities offered by System Security and Audit Trails—to meeting the user accountability requirements of MFG/PRO customers with regulated environments.

Eligible Programs

◆ See “Profiles” on page 297.

Electronic signature functionality is limited to a subset of MFG/PRO programs, tables, and fields that are defined in QAD-provided default signature profiles. Table 9.1 lists the programs that currently can have electronic signatures enabled.

Table 9.1
Programs Included
in Default Profiles

MFG/PRO Module	Menu	Program
Product Change Control (PCC) ¹	1.9.6.1	PCR/PCO Approval
	1.9.6.13	Detail Approval Maintenance
	1.9.7.4	Incorporation Selection
	1.9.7.5	Incorporation
	1.9.7.13	Implementation
Compliance	1.22.1	Lot Master Maintenance
	1.22.24	Compliance Control
Inventory Control	3.1.1	Inventory Detail Maintenance
	3.1.2	Detail Maintenance by Item/Lot
	3.4.1	Transfer—Single Item
	3.4.3	Transfer With Lot/Serial Change
	3.4.4	Batchload Transfer with Lot/Serial Change
	3.24	Inventory Control
Shop Floor Control	17.1	Labor Feedback by Work Order
	17.2	Labor Feedback by Employee
	17.3	Labor Feedback by Work Center
	17.4	Non-Productive Labor Feedback
	17.5	Operation Complete Transaction
	17.6	Operation Move Transaction
Quality Management	19.11	Quality Order Results Entry
	19.13	Test Results Maintenance

1. Along with the addition of electronic signatures, PCC has also been enhanced to improve overall security and accountability. See “Product Change Control” on page 39 for a summary of these changes.

Various reports and inquiries associated with signature-eligible menu programs can display signature data. The field that controls this feature—Display E-Signature Details—displays on the user interface based on setup data.

► See “Functional Reports and Inquiries” on page 328.

The electronic signature function prompts for and maintains signature information based on signature profiles. Each profile is associated with a specific category of data and indicates whether signatures should be captured and for which menu programs, as well as which fields are being signed.

Important Categories are defined by QAD and delivered with the electronic signature functionality. Adding new categories requires custom development.

Electronic Signatures Work Flow

Use the programs on the E-Signature Setup Menu (36.12.14) to set up and configure electronic signature functions. Figure 9.1 illustrates the electronic signature process work flow; use it to set up signature functions in your environment.

Fig. 9.1
Electronic
Signatures
Setup Flow

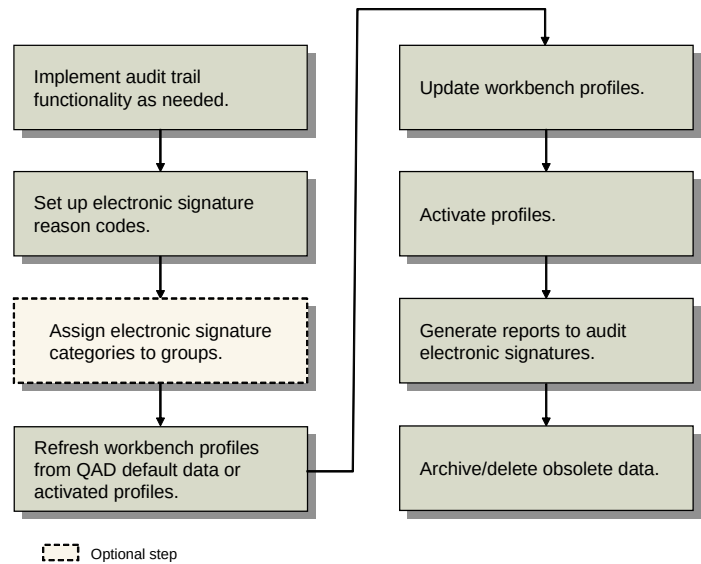


Table 9.2 shows the programs available for setting up and reporting on electronic signature functions.

Table 9.2
Electronic
Signatures
Programs

Menu Number	Description	Program Name
36.12.4	E-Signature Events Report	esevtrp.p
36.12.5	E-Signature History Report	eshstrp.p
36.12.7	E-Signature Failure Report	esflrp.p
36.12.14.1	E-Signature Group Maintenance	escgmt.p
36.12.14.2	E-Signature Group Report	esgrrp.p
36.12.14.4	E-Signature Workbench Refresh	eswpref.p

Menu Number	Description	Program Name
36.12.14.5	E-Sig Workbench Profile Maint	eswpmt.p
36.12.14.6	E-Sig Workbench Profile Report	eswprp.p
36.12.14.8	E-Signature Profile Activation	eswpact.p
36.12.14.9	Activated E-Sig Profile Report	esacrp.p
36.12.14.11	E-Sig Category Master Report	escatrp.p
36.12.14.21	E-Sig Failure Archive/Delete	esesigup.p
36.12.14.22	E-Signature Archive/Delete	esesup.p
36.12.14.23	E-Signature Restore	esesld.p

Before electronic signature processing can begin, the prerequisite planning and implementation steps must be completed:

- Planning steps include:
 - Determine the types of data that need to be signed based on the regulatory requirements for your specific industry or environment.
 - Determine how MFG/PRO fits into your overall business processes, as well as which specific electronic signatures support those processes.
 - Complete data mapping requirements for records and available signatures.
 - Determine audit trail and security requirements for signed records; for example, assign menu security to prevent users who should not sign records from accessing the programs that require signatures.

Note Electronic signatures should be part of a detailed security plan to meet your overall business requirements.

- Implementation steps include:
 - Define reason codes to explain the meaning of each signature.
 - Optionally, define electronic signature groups to simplify the setup process.
 - Load QAD-provided default signature profiles and modify them as needed, setting appropriate filter criteria.
 - Activate the updated profiles.

The first activity in setting up electronic signature functions is to plan the extent to which you need to require signatures. Regulatory agencies are often specific about the types of data that must be signed, as well as the role of the signing individual—verifier, approver, and so on. Before you start the implementation, be sure that your signatures meet the needs of the appropriate regulatory agency. While MFG/PRO offers a range of programs, tables, and fields that can be included in signature processing, you might not be required to implement more than a few.

◆ See page 302.

A critical component of virtually any electronic signature is the signature meaning—whether the person applying the signature was approving, inspecting, reviewing, or so on. In MFG/PRO, the reason code provides the signature meaning. Be sure to plan and implement reason codes that make sense in your specific regulatory environment.

◆ See page 305.

To avoid repetitive data entry for individual category profiles, create *signature groups* in E-Signature Group Maintenance (36.12.14.1). An electronic signature group is a group of category profiles that can be managed at the same time. A *category* is the definition of a set of MFG/PRO data that can be signed as a unit. Creating an electronic signature group removes the requirement that each category profile must be refreshed or activated individually. When a group is refreshed or activated, profiles for all member categories are automatically updated. This saves time and can be used to organize categories into functionally similar groups.

◆ See page 315.

To begin requiring electronic signatures, activate the profiles with E-Signature Profile Activation (36.12.14.8). Activated profiles are staged to begin on a future date; signature recording does not occur immediately after a profile is activated. On the specified begin date, the system begins requiring and recording signature data as defined by each profile.

◆ See page 324.

Use E-Signature Events Report (36.12.4) and E-Signature History Report (36.12.5) to view information that applies to electronic signatures. Use E-Signature Failure Report (36.12.7) as part of your security program to identify potential unauthorized access attempts.

Categories

A category is a QAD-provided definition of a set of MFG/PRO data that can be signed as a unit in certain menu programs. For example, it identifies a set of tables and fields, as well as the menu program or programs from which this data can be signed.

Because records in a given MFG/PRO table can be updated by more than one program, a category can be associated with more than one menu program. Conversely, a program can update more than one table; multiple categories can apply to a single menu program.

Example The Operation History category (0003) generates signatures for tables and fields that store operation history information. Since these tables can be updated from several Shop Floor Control (menu 17) programs, several programs are included in the category. Because those same programs can also update records associated with quality results, they are included in the Quality Results category (0002) as well.

Users cannot update category definitions. Instead, QAD provides a default *profile* for each category. You can refresh the workbench profiles with these defaults and modify them based on the specific needs of your environment.

Category definitions include a default set of *filters* that can be used to determine whether a signature is required based on a given value for a site, item number, or other data element. Although filters are defined for each category, their use is optional; control how filters apply to your implementation by updating the category profile using the workbench.

◆ See “Filters” on page 300.

Table 9.3 lists the electronic signature categories, as well as the default menu programs associated with them. If for some reason you do not want a particular program to generate electronic signatures, you can deselect it in the workbench profile.

◆ See “Apply Profile to Menu Programs” on page 312.

Table 9.3
QAD-Defined
Categories

Code	Name	Description	Available Menu Programs
0001	InvCtrl	Inventory Control	Inventory Control (3.24)
0002	QualRes	Quality Results	Labor Feedback by Work Order (17.1) Labor Feedback by Employee (17.2) Labor Feedback by Work Center (17.3) Operation Move Transaction (17.6)
0003	OpHist	Operation History	Labor Feedback by Work Order (17.1) Labor Feedback by Employee (17.2) Labor Feedback by Work Center (17.3) Non-Productive Labor Feedback (17.4) Operation Complete Transaction (17.5) Operation Move Transaction (17.6)
0004	ComCtrl	Compliance Control	Compliance Control (1.22.24)
0005	LotMstr	Lot Master	Lot Master Maintenance (1.22.1)
0006	InvDet	Inventory Detail	Inventory Detail Maintenance (3.1.1) Detail Maintenance by Item/Lot (3.1.2)
0007	InvTran	Transaction History	Inventory Detail Maintenance (3.1.1) Detail Maintenance by Item/Lot (3.1.2) Transfer—Single Item (3.4.1) Transfer with Lot/Serial Change (3.4.3) Batchload Transfer with Lot/Serial Change (3.4.4) Quality Order Results Entry (19.11)
0008	QualOrd	Quality Order	Quality Order Results Entry (19.11) Test Results Maintenance (19.13)
0009	PCOInc	PCO Incorporation	Incorporation Selection (1.9.7.4) Incorporation (1.9.7.5) Implementation (1.9.7.13)
0010	PCOAppr	PCO Approval	PCR/PCO Approval (1.9.6.1) Detail Approval Maintenance (1.9.6.13)

Note Some categories are also associated with reports and inquiries that can include electronic signature data. See “Functional Reports and Inquiries” on page 328 for information.

Use E-Sig Category Master Report (36.12.14.11) to view information about the QAD-defined categories.

Category 0007 Considerations

Current signature data for category 0007, Transaction History, is never shown as part of the latest electronic signature when you access a previously signed record from one of the programs listed in Table 9.3 for category 0007. When setting up this category, you should ensure that the fields and filters selected match for programs associated with two categories—such as Inventory Detail Maintenance—to avoid confusion regarding which data the signature is applied to.

▶ See “Recording Electronic Signatures” on page 316.

Note You can still view the final data being signed in the final signature data frame for this category.

Profiles

The electronic signature system maintains signature information based on a signature profile that is associated with a specific category of data. The category profile specifies:

- Whether electronic signatures are required
- In which programs
- Which fields are signed
- Characteristics of how signatures are displayed and recorded
- Filter definitions

Tip
Profiles are identified by the corresponding QAD-defined category codes.

The life cycle of a profile consists of three phases:

- The QAD-provided default profile. Based on QAD-provided category data, this is loaded when you install Enhanced Controls and serves as the template for profiles used by the system. You cannot update default profile records directly—only after you have copied them by refreshing the workbench profiles.

▶ See “Refreshing Signature Profiles” on page 306.

Note You can view the structure of default profiles without refreshing the workbench. Use E-Sig Workbench Profile Report (36.12.14.6) with Display Default Profile set to Yes.

- The workbench profile. This is initially based on the corresponding default profile for a given category. It is an intermediate working version used to tailor each profile for specific requirements. You can refresh it based on an existing activated profile or the default profile.

▶ See “Updating Signature Profiles” on page 308.

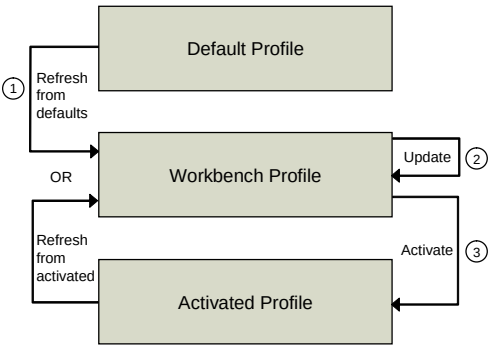
Because the workbench profile has no effect on current system activities, you can continue to update it while the active version controls electronic signature processing.

See “Activating Electronic Signature Profiles” on page 315.

- The activated profile. This is the profile used by the system to control electronic signature processing. It is copied from the workbench profile during activation along with a begin date, and it stays in effect until the begin date of another active profile for the same category.

Figure 9.2 summarizes the relationships between the three category profile types.

Fig. 9.2
Profile Flow



Tables and Fields

See “Updating Signature Profiles” on page 308.

The category profile includes a list of tables and fields that define the data to be signed in the corresponding signature-enabled programs.

Each category profile includes one or more database tables and their corresponding set of fields. For example, the profile for category 0007, Transaction History, includes fields from the inventory transaction history table (tr_hist). In some cases, a category profile might include multiple tables where the records are related in a hierarchy of parent-child relationships. For example, a table might have associated child records in the transaction comments (cmt_det) table.

Greater-than symbols (>) and spaces show the hierarchical relationships among tables and fields on the list. Top-level tables are preceded by a single > symbol; fields within the table begin with a > symbol and a

space. Tables with child relationships are designated with an additional > symbol; fields in child tables include the same number of > symbols as the corresponding tables, again with a space separator.

Example Figure 9.3 shows a portion of the default profile structure for category 0002, Quality Results, which specifies the test results data to be signed in several programs in Shop Floor Control (menu 17). View default profiles using E-Sig Workbench Profile Report (36.12.14.6) with Display Default Profiles set to Yes.

Parent-level table			Sel Type	Name - Label

Field in parent-level table	Yes	Table	☒	mph_hist - Master Specification Test History
	No	Field	☒	oid_mph_hist - * MPH_HIST
	No	Field		> mph_attribute - Attribute
	No	Field		> mph_cmtindx - Comment Index
	No	Field		> mph_date - Test Date
	No	Field		> mph_domain - Domain
	No	Field		> mph_lot - ID/Batch
	No	Field		> mph_mch - Machine
	No	Field		> mph_op - Operation
	No	Field		> mph_op_trnbr - Transaction Number
	No	Field		> mph_part - Item Number
	No	Field		> mph_pass - Pass
	No	Field		> mph_procedure - Document
	No	Field		> mph_routing - Routing/Procedure
	No	Field		> mph_result - Results
	No	Field		> mph_test - Characteristic
	No	Field		> mph_testmthd - Test Method
Child-level table	Yes	Table	☒	cmt_det - Transaction Comments
	No	Field	☒	oid_cmt_det - * CMT_DET
	No	Field		>> cmt_cmmt - Comment Data
	No	Field		>> cmt_domain - Domain
Field in child-level table				

Fig. 9.3
Example of
Workbench Profile
Table/Field
Structure

Top Tables

Each QAD-provided category definition includes a top-level table, which displays in the Top Table field in the first frame of E-Sig Workbench Profile Maintenance. In most cases, this is the first table that appears in the profile structure.

In other cases, however, the top table is not included in the data to be signed but instead provides key values for identifying the signed data.

Example The top table in the Quality Results category is the work order routing (wr_route) table, but this table is not included in the data to be signed; that consists of the master specification history (mph_hist) table and related transaction comments (cmt_det). The wr_route record is used only to identify the signed data by providing the context.

◆ See “Electronic Signature Reports” on page 324.

You can specify top-table field values to identify MFG/PRO data that may have signatures attached; for example, use E-Signature History Report (36.12.5) to view signature history associated with a specific work order identified in the wr_route table.

Filters

Depending on the specific requirements of your environment, you may not need to record electronic signatures for all records of a given type. For example, you might want to require signatures only on inventory transactions involving a specific site or certain items.

QAD-provided categories include filters for selecting or excluding data that must have electronic signatures applied.

Table 9.4 indicates the filters that are available in each QAD-provided category definition.

Table 9.4
Available Filters,
by Category

Category	Filter				
	Domain	Site	Item Number	Location	Work Center
0001 Inventory Control	✓				
0002 Quality Results	✓	✓	✓		✓
0003 Operation History	✓	✓	✓		✓
0004 Compliance Control	✓				
0005 Lot Master	✓		✓		
0006 Inventory Detail	✓	✓	✓	✓	
0007 Transaction History	✓	✓	✓	✓	
0008 Quality Order	✓	✓	✓	✓	

Category	Filter				
	Domain	Site	Item Number	Location	Work Center
0009 PCO Implementation	✓				
0010 PCO Approval	✓				

When you refresh a workbench profile based on the QAD-provided default profile, the filter mode is set to indicate that filtering will not be applied. If you choose to set up signature requirements based on available filters, specify appropriate values when you define your implementation-specific profile in E-Signature Workbench Profile Maintenance.

◆ See “Set Up Filters” on page 314.

Filters are designed to work either by inclusion or exclusion, as defined by the Filter Mode field in E-Signature Workbench Profile Maintenance. For example, an *inclusion* filter might be set up to include records by site and location. If you set up the filter criteria with site values of 1000 and 2000 and location values of loc1 and loc2, only records with a combination of one of those sites and one of those locations will require an electronic signature. In this scenario, updating a record associated with site 1000, loc3 would not trigger a prompt for an electronic signature.

Tip
A profile can have either inclusion or exclusion filters—but not both.

In the same example, defined as an *exclusion* filter, electronic signatures would not be required for records with any combination of the specified sites and locations. Updates to records with any other sites and locations, however, would trigger a signature prompt.

Completing Prerequisite Activities

Before you start setting up records that control when electronic signatures are required and how they are recorded, you should complete the following tasks:

- Set up audit trail functionality
- Define signature reason codes
- Check Security Control settings

Set Up Audit Trails

Although electronic signature functions can be used without Audit Trails—signature data is stored in production database tables rather than in the audit database—this is not a typical business case. Signatures normally fill only part of the user accountability requirements of a regulated environment. Other important elements supported by MFG/PRO are:

- Access security control and tracking, provided by the System Security module
- The ability to identify changes to the database, as well as identify who made them—the primary function of Audit Trails

Additionally, as part of the overall accountability process, electronic signature records cannot be deleted unless they are first archived to an audit database. If you ever want to delete signature records, you must have at least one audit database in place and connected.

◆ See “Setting Up Database Connections” on page 263.

For the audit database you will use for signature archive, set E-Signatures to Yes and specify an associated begin date in Audit DB Maintenance (36.12.13.11). This is the database used for archiving electronic signature records. Whether you use the same database that stores audit trail records should be determined as part of your overall audit database planning.

Define Signature Reason Codes

The signature reason code is a critical element of the electronic signature. In regulatory environments, the signature record typically must include the meaning of the signature. In MFG/PRO, the reason code provides the meaning.

◆ See “Recording Electronic Signatures” on page 316.

Each time the system prompts for an electronic signature, the user must provide a valid reason code. For example, reason codes might indicate that a quality record has been approved, reviewed, or inspected.

Use Reason Codes Maintenance (36.2.17) to define signature reason codes that are appropriate to your environment.

Important All reason codes used by electronic signatures must be associated with the QAD-provided ESIG reason type. Reasons of any other type cannot be entered in the signature prompt frame.

Review Security Control Settings

To guard against attempts by unauthorized individuals to apply electronic signatures using another user's ID, signature validation logic is similar to that used in the MFG/PRO log-in process.

Review Security Control (36.3.24) to see how log-in security is defined in terms of password structure and use rules.

► See Chapter 7, “Users and Security,” on page 193 for information on setting up and using log-in security.

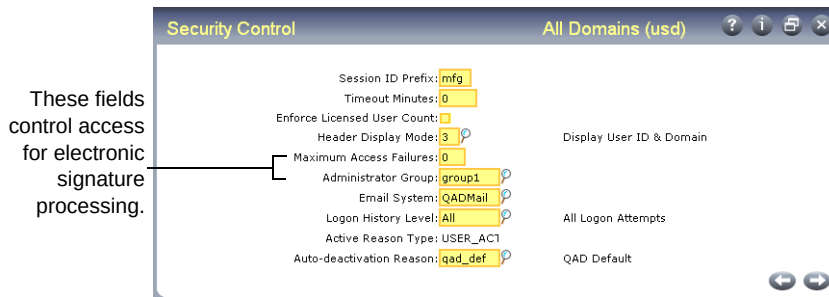


Fig. 9.4
Security Control
(36.3.24)

Two fields directly control how the system manages unsuccessful electronic signature attempts:

- Max Access Failures indicates how many consecutive unsuccessful signature attempts cause the user's MFG/PRO session to terminate, deactivate the account, and inform the administrator group of a potential unauthorized access attempt.
- Administrator Group is the name of the user group—defined in User Group Maintenance (36.3.4)—whose members are notified by e-mail when a session is terminated because of excessive unsuccessful signature attempts. The system also sends e-mail to this group when a signature profile is activated.

► See “E-Mail Notifications” on page 321.

Defining Electronic Signature Profiles

Setting up and using electronic signature profiles include these steps:

- Create electronic signature groups.
- Refresh workbench profiles.
- Update workbench profiles.
- Activate profiles.

Overview

Each category is associated with one or more signature-eligible MFG/PRO programs in its own profile. Initially, all signature profiles are empty; they must be refreshed with the QAD-provided information. Category profiles hold values that electronic signature functions use to manage the information retention and reporting process. This information affects electronic signature functions only after the profile is activated.

A category profile:

- Indicates whether signature functions are enabled for the category in general and for specific menu programs.
- Specifies control information that determines how electronic signature data displays when an enabled program runs.
- Maintains a list of tables and fields that defines the data to be signed. This data is included in signature records.
- Defines filters that can be used to determine whether electronic signature requirements apply to all records or only those containing specified values.

► See “Profiles” on page 297.

The system maintains three sets of profiles: the QAD-supplied default profiles, the profiles you edit in the workbench, and the activated profiles. When you activate a profile, the system creates a new activated profile by copying your completed workbench profile and setting the begin date. Since the system activates a copy of your workbench profile, you can continue to modify the workbench profile with E-Signature Workbench Profile Maintenance without affecting the active system.

Before refreshing workbench profiles, you can optionally create signature groups to manage several profiles more easily and streamline the data setup process. Once refreshed, modify the workbench profiles with your requirements. You can enable or disable signatures and update filters as needed. When your workbench profiles are complete, activate them and set a begin date. To discontinue signatures, simply update the workbench profile to set E-Signature On to No; then activate it with the begin date set to the date signatures are no longer needed.

Creating Signature Groups

Use E-Signature Group Maintenance (36.12.14.1) to group all the categories you plan to control using electronic signatures, or to group related categories for signature purposes. Signature groups streamline the setup process by letting you refresh and activate the profiles for all member categories at once, instead of one profile at a time.

Example You might create a group called Control that includes the Inventory Control (0001) and Compliance Control (0004) categories so that you can refresh and activate both control program-related profiles at the same time.

The screenshot shows the 'E-Signature Group Maintenance' window for 'All Domains (usd)'. It has three main sections:

- Group Information:**
 - Group Name: all
 - Description: all groups
- Group Detail:** A table listing categories assigned to the group.

Category Code	Category Description
0001	Inventory Control
0002	Quality Results
0003	Operation History
0004	Compliance Control
0005	Lot Master
0006	Inventory Details
0007	Transaction History
- Cross Reference Maintenance:**
 - Category Code: 0001
 - Description: Inventory Control

Navigation buttons (back, forward, delete) are at the bottom right.

Fig. 9.5
E-Signature Group
Maintenance
(36.12.14.1)

Specify a group name, up to eight characters. An electronic signature group cannot have the same name as a category code.

Next, provide a brief description and choose Go to display the Group Detail frame, which lists all the categories currently assigned to the group. Use the Cross Reference Maintenance frame to add or delete categories.

Use E-Signature Group Report (36.12.14.2) to display the records defined in this program.

Refreshing Signature Profiles

When initially setting up electronic signature functions, workbench category profiles are empty and must be manually populated. Use E-Signature Workbench Refresh (36.12.14.4) to update the empty profiles with the QAD-provided default information. You can refresh one category at a time or, optionally, refresh the profiles for an entire group of categories.

You can use this program later to restore the QAD-provided default data, modified in E-Signature Workbench Profile Maintenance, or to update workbench profiles based on existing active profiles.

Note Any changes you make with this program do not affect activated profiles currently in use.

Fig. 9.6
E-Signature
Workbench Refresh
(36.12.14.4)



Tip
If Value is blank,
the system prompts
you to confirm.

Indicate if you want to refresh categories or groups; then use the Value field to specify the category name or group name to be refreshed. Leave Value blank to refresh all categories or groups, based on the setting in the Group/Category field.

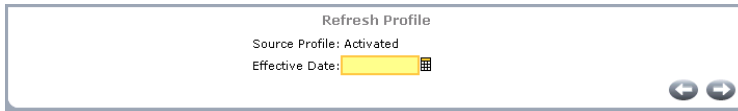
Use the following field descriptions to enter the values for the refresh process.

Refresh Profiles. Indicate whether to refresh all data for the specified profiles. When this field is Yes, an additional frame displays that you can use to determine which profiles are used as the source of the updates.

Override Fields. Indicate whether to override the field that controls electronic signatures for the specified profiles. When this field is Yes, an additional frame displays.

Refresh Profile Frame

If Refresh Profiles is Yes, the Refresh Profile frame displays.



The image shows a rectangular frame titled "Refresh Profile". Inside the frame, the text "Source Profile: Activated" is displayed. Below it, the text "Effective Date:" is followed by a yellow rectangular input field and a small calendar icon. In the bottom right corner of the frame, there are two circular arrows, one pointing left and one pointing right.

Fig. 9.7
E-Signature
Workbench
Refresh, Refresh
Profile Frame

Source Profile. Enter Activated or Default to indicate which profiles to use as the source for refreshing the profiles selected previously.

Activated: Each specified workbench profile is refreshed using the activated profiles in use on the date specified in Effective Date. The corresponding profiles must be in use on the date specified; otherwise, the system displays an error for each activated profile not found and the refresh does not occur for that profile.

Default: Each specified workbench profile is refreshed using the QAD-provided values. Select this value when initially setting up electronic signature functions to load the QAD-provided values into the profiles for the categories in which you plan to use signatures.

Effective Date. Enter a date when the activated source profile was in use. The workbench profile is refreshed using the active source profile settings in use on this date. If an activated profile was not in use on the specified date, an error displays and the target profile is not refreshed.

Example Enter today's date to refresh the workbench profiles based on the activated profiles currently being used.

Tip
This field is
available only when
Source Profile is
Activated.

Override Fields Frame

If Override Fields is Yes, the Override Fields frame displays.



The image shows a rectangular frame titled "Override Fields". Inside the frame, the text "E-Signature On:" is followed by a checked checkbox. In the bottom right corner of the frame, there are two circular arrows, one pointing left and one pointing right.

Fig. 9.8
E-Signature
Workbench
Refresh, Override
Fields Frame

E-Signature On. Indicate whether to enable electronic signature functions for the profiles being refreshed.

If Refresh Profiles is No, the value specified here replaces the E-Signature On value in the current workbench profiles for the specified group or category. However, no other workbench data is updated.

When you refresh based on QAD-provided profiles, signature functions are turned on by default. You can use this field to override that setting.

Use E-Signature Workbench Profile Maintenance to change this value for individual profiles.

Updating Signature Profiles

Use E-Signature Workbench Profile Maintenance (36.12.14.5) to adjust profile settings for your specific environment by:

- Defining control settings that determine how electronic signature processing works for each category
- Specifying the menu programs from the available list where signatures will be applied to the category
- Updating the list of tables and fields that are to be signed and included in signature records
- Setting up filters to control whether specific data is subject to or exempt from signature requirements

◆ See “Activating Electronic Signature Profiles” on page 315.

To disable electronic signatures for a profile that currently requires them, you must create a new activated profile for the category. Do this by updating the workbench profile and setting the E-Signature On value to No; then activate that new profile with the proper begin date.

Use E-Signature Workbench Profile Report (36.12.14.6) to display the information updated in this program.

◆ See page 297 for information.

Note Some special considerations apply when you are setting up profiles that involve category 0007, Transaction History.

Specifying Control Settings

Figure 9.9 illustrates the first frame of E-Signature Workbench Profile Maintenance.

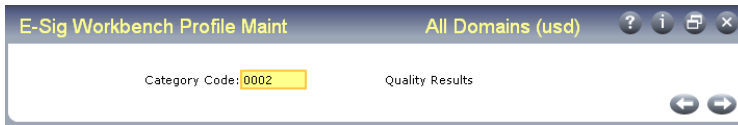


Fig. 9.9
E-Signature
Workbench Profile
Maintenance
(36.12.14.5)

Enter a QAD-defined category code and choose Go. The system displays several fields you can use to control electronic signature processing.

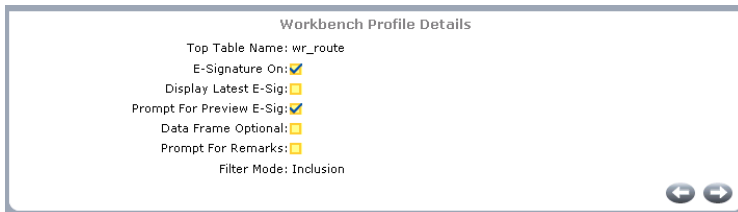


Fig. 9.10
E-Signature
Workbench Profile
Maint, Workbench
Profile Details

Top Table Name. The system displays the name of the table used to identify the set of data defined by the category; this sets the context for the signed data.

Example Category 0002, Quality Results, has a value of wr_route (work order routing) in this field. Master specification test history (mph_hist) is shown as the first table in the 0002 profile structure. One electronic signature could contain many records of this type—so the mph_hist identification is not unique. However, all mph_hist records from the electronic signature instance are related to a single wr_route record, which serves as a unique identifier for the signed data.

E-Signature On. Indicate whether the system should apply the electronic signature functions for the category defined in this profile when it is activated.

No: Electronic signatures do not apply to this category. Use this option to turn electronic signatures off for programs that currently require them. For example, if signatures are currently used and a new profile for this category with E-Signature On set to No is activated, electronic signature functions stop on the new profile's begin date.

Yes: Once this profile is activated, electronic signatures are required for this category as defined by the menu details and applicable filters.

When you refresh from QAD-provided default data, the value is Yes.

See “Tables and Fields” on page 298.

◆ See “Recording Electronic Signatures” on page 316.

Tip
This feature does not apply to all signature-enabled programs.

◆ Figure 9.17 on page 318 shows the frame that displays when this field is Yes.

Display Latest E-Sig. Indicate whether the system displays the latest electronic signature when programs controlled by this profile are executed.

When you refresh from QAD-provided default data, the value is Yes. Figure 9.16 on page 317 shows the frame that displays when this field is Yes.

Prompt for Preview E-Sig. For programs that generate transactions, enter Yes to have the system prompt for a signature before the transaction data is created. The user is given the option to display the final data before signing. You can use this feature to avoid potential record-locking issues.

When the user sets Show Final Data to Yes when entering a signature, the system creates the transactions and displays final data before it is signed. Otherwise, the user enters the signature without viewing the final data.

When you refresh from QAD-provided default data, the value depends on the types of programs included in the category.

This configurability is provided to address record-locking issues that might be caused by the user interacting with the signature frame. In some menu programs that create transaction records such as operation or transaction history, the system locks frequently updated records while creating the transaction records. These programs have been designed to minimize the amount of time that records are locked by having no user interaction during record creation.

When electronic signatures are used with these programs and the final data to be signed—including the transaction data—must be displayed to the user while prompting for the signature, records remain locked until the user successfully completes the signature. This record-locking during signing is necessary because all changes must be rolled back if the signature is not accepted. During this time, no other users can update these same locked records. This issue becomes even more problematic, for example, if the user decides to take a break at this crucial time, before entering the signature fields.

This problem can be avoided in most situations because the relevant data for the user to review before signing are the fields that the user entered. These fields are generally available in the preview signature frames. After the signature is accepted, the program generates the

transaction records and includes them in the signed data stored with the signature. Your system validation process can provide the assurance that the program systematically and reproducibly generates the transaction records based on the entered data. So, by signing in the preview signature frame, the final data never needs to be displayed and the records will not be locked any longer than required to create them. If the signature is not accepted, all user changes are rolled back and the transaction records are not created.

Set Prompt for Preview E-Sig to Yes to avoid these potential problems.

Data Frame Optional. Enter Yes to allow users to immediately enter an electronic signature without scrolling through the data to be signed. In this case, they can still view all the fields by setting Scroll Details to Yes in the signature frame.

◆ See Figure 9.17 on page 318.

When the field is No, focus is on the frame that displays the data to be signed. To enter the signature, users must first choose End to exit that frame.

When you refresh from QAD-provided default data, the value is Yes.

Prompt for Remarks. Indicate whether the user can add an optional remark while entering electronic signature data. When this field is Yes, a 64-character updateable Remarks field displays in the signature frame. Remarks are included in the electronic signature record.

When you refresh from QAD-provided default data, the value is Yes.

Filter Mode. Specify the type of filtering the system will use in determining whether specific data requires electronic signatures.

◆ See “Filters” on page 300.

None: Filters are not used. The Filters and Filter Criteria frames do not display.

Inclusion: Only data meeting the specified filter criteria requires electronic signatures.

Exclusion: All data except those meeting the specified filter criteria require electronic signatures.

When you refresh from QAD-provided default data, the value is None.

Tip
A profile can have either inclusion or exclusion filters—but not both.

Multiple Categories

Based on the data they update, some menu programs can be associated with more than one category. When this occurs, the system includes logic to resolve conflicting workbench profile setup data for three settings:

- Prompt for Preview E-Sig
- Data Frame Optional
- Prompt for Remarks

Table 9.5 shows the sequence the system uses for determining which profile takes precedence in each such case.

Note This logic is needed only when a program is selected in the Workbench Profile Menu Details frame of more than one category profile. Additionally, when the menu program is executing, if a signature is not required for the first category, the second category profile is used to determine these three settings.

Table 9.5
Profile Precedence
for Multiple
Categories

Menu Program	Category Sequence
Labor Feedback by Work Order (17.1) Labor Feedback by Employee (17.2) Labor Feedback by Work Center (17.3) Operation Move Transaction (17.6)	1. Operation History (0003) 2. Quality Results (0002)
Quality Order Results Entry (19.11)	1. Transaction History (0007) 2. Quality Order (0008)

Apply Profile to Menu Programs

When you initially set up electronic signature functions by refreshing profiles based on QAD-provided data, each category is associated with one or more MFG/PRO menu programs that update the data defined in the category.

Although you cannot specify additional programs, you can use the Workbench Profile Menu Details frame to control whether signature functionality will apply to the available menu programs.

When a program is included in the category profile, an asterisk (*) displays in the Apply column. Clear the field to deselect a program.

Note If a program appears more than once in the menu system, the frame lists all menu numbers. Changing the Apply setting for one menu number automatically updates all.

In some profiles, the program list includes reports and inquiries. These programs can display signature data if included in the activated profile. When they are included, they have a Display E-Signature Details field that gives the user the option of displaying signature data in the output.

See “Functional Reports and Inquiries” on page 328.

Workbench Profile Menu Details			
Apply	Menu Item	Menu Label	Execution File
*	17.1	Labor Feedback by Work Order	sfoptr01.p
*	17.13.14	Operations by Work Order Report	sfopr12.p
*	17.13.15	Operations by Employee Report	sfopr13.p
*	17.13.9	Operation Transaction Detail Inq	sfopiq12.p
*	17.2	Labor Feedback by Employee	sfopr02.p
*	17.3	Labor Feedback by Work Center	sfopr03.p
*	17.6	Operation Move Transaction	sfopr06.p
*	19.13	Test Results Maintenance	mptrmt.p
*	19.15	Test Results Report	mpcarp.p

Fig. 9.11
E-Signature
Workbench Profile
Maint, Workbench
Profile Menu
Details

Select Tables and Fields

QAD-provided setup data includes a set of tables and fields that define the data to be signed and stored with the signature. The Workbench Profile Structure frame lists the tables and fields defined by the category.

If the current profile was refreshed based on default data, all tables and fields are selected.

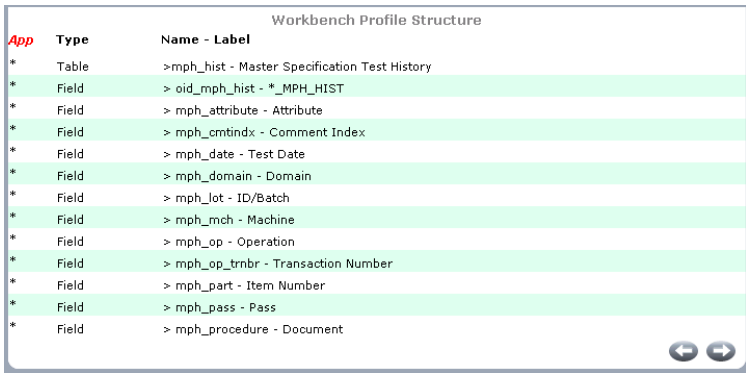
Toggle the asterisk in the Sel column to select or deselect fields or tables. If you deselect or select a table, all fields in the table are automatically deselected or selected as well. In that case, the frame display does not refresh immediately.

Note The first field listed for each table is the system-assigned object ID (OID) that uniquely identifies each record in the database. You cannot deselect this field.

The system uses greater-than symbols (>) and spaces to show the hierarchical relationships between table and field elements in the profile structure.

See “Tables and Fields” on page 298.

Fig. 9.12
E-Signature
Workbench Profile
Maint, Workbench
Profile Structure



App	Type	Name - Label
*	Table	>mph_hist - Master Specification Test History
*	Field	> oid_mph_hist - *_MPH_HIST
*	Field	> mph_attribute - Attribute
*	Field	> mph_cmtindx - Comment Index
*	Field	> mph_date - Test Date
*	Field	> mph_domain - Domain
*	Field	> mph_lot - ID/Batch
*	Field	> mph_mch - Machine
*	Field	> mph_op - Operation
*	Field	> mph_op_trnbr - Transaction Number
*	Field	> mph_part - Item Number
*	Field	> mph_pass - Pass
*	Field	> mph_procedure - Document

Set Up Filters

When Filter Mode is Inclusion or Exclusion in the Workbench Profile Details frame, additional frames let you select and set up filters. Filter frames do not display when Filter Mode is None.

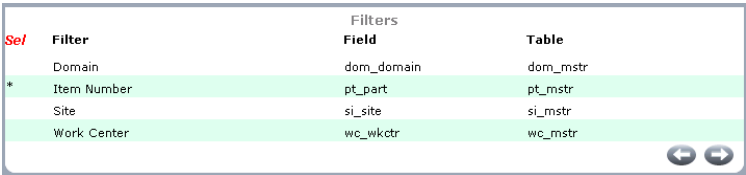
◆ See “Filters” on page 300.

These settings determine whether electronic signature processing occurs for data associated with specified values.

Use the Filters frame to specify which of the available filters you want to apply to this category profile. When the Sel column includes an asterisk, the filter is selected and displays in the Filter Criteria frame

Note You cannot complete the profile record if all selected filters do not have at least one criteria value. The system prompts you to remove such filters from the profile.

Fig. 9.13
E-Signature
Workbench Profile
Maint, Filters



Sel	Filter	Field	Table
	Domain	dom_domain	dom_mstr
*	Item Number	pt_part	pt_mstr
	Site	si_site	si_mstr
	Work Center	wc_wkctr	wc_mstr

The Filter Criteria frame lists all the filters that were selected in the Filters frame. To enter criteria values for a filter, navigate to the Criteria Value frame and enter a value that will be used to either include or exclude electronic signature processing, depending on the filter mode.

You cannot enter data ranges for a filter. Instead, enter multiple criteria values. Each criteria value displays on a separate line in the Filter Criteria frame.

To filter on a blank value, enter the filter field name and leave Value blank. The system prompts you to confirm. A blank value is not a wildcard; instead, it only matches data where the value is actually blank.

Important Since the system does not validate this value, you should exercise caution when you set up filters. For example, if you are setting up an inclusion filter to require electronic signatures only for a single site and accidentally enter an invalid site code, the program will never prompt for a signature.

Fig. 9.14
E-Signature
Workbench Profile
Maint, Filter
Criteria and Value

Activating Electronic Signature Profiles

After completing the workbench profiles, use E-Signature Profile Activation (36.12.14.8) to activate profiles for one category or a group of categories. Activated profiles are staged for electronic signature functions to begin on a future date; signature settings are not in effect immediately after a profile is activated.

Fig. 9.15
E-Signature Profile
Activation
(36.12.14.8)

Leave Value blank to include all groups or categories.

Profiles cannot be activated on the begin date. Plan all changes ahead of time and activate updated profiles before their begin date. Profiles must have the begin date set to sometime in the future. Activated profiles become effective at 12:00 AM on the specified date.

You can execute this program in batch mode if you are activating a group with many associated categories.

When this program completes execution, it generates a report that displays information for each activated profile. The report includes the following for both the original profile and the newly activated one:

- The category name.
- The value of E-Signature On.
- The begin date.
- The data structure of the profile, listing all tables and fields that are marked as selected in E-Signature Workbench Maintenance. The system uses greater-than symbols (>) and spaces to show the hierarchical relationships between data elements.

◆ See “Tables and Fields” on page 298.

If Activate Profiles is No, only the report is generated; the profiles currently in use are not updated. You can use this setting to verify the effects of running the program before you actually activate the profiles.

Use Activated E-Sig Profile Report (36.12.14.9) to display details about activated profiles.

◆ See “E-Mail Notifications” on page 321.

When a profile is activated, the system automatically sends an e-mail message to members of the administrator group specified in Security Control (36.3.24).

Recording Electronic Signatures

When profiles with E-Signature On set to Yes have been activated using E-Signature Profile Activation and the specified begin date is reached, the system automatically begins prompting for electronic signatures based on rules defined in the active profile.

When Display Latest E-Sig is Yes in the active profile, before displaying MFG/PRO data defined by the category, the system displays the signature that was recorded most recently for that data. For example, Figure 9.16 shows the latest signature for Labor Feedback by Work Order (17.1).

Note Latest signature data for category 0007, Transaction History, is not included in the display for programs associated with that category.

◆ See page 297.

Indicates whether any values have been modified since record was signed.

Fig. 9.16
Latest Electronic
Signature Display

The top frame of a signature display includes such information as the user ID and name of the person who applied the signature and the associated reason code.

The signature display also includes a Current field, which indicates if all the signed data fields recorded at the time of the signature still have the same values. If an included field has been updated since the record was signed—for example, with another program that is not signature enabled—the system sets Current to No.

Note The Current setting is not stored as part of the signature instance. It is determined in real time based on the activated profile currently in effect. If multiple categories are signed in one menu program, each category of signed data is independent of the others. If the data changes in one, it does not affect the Current setting of the others.

The lower frame shows the value of the signed data fields at the time of the last signature. Greater-than symbols (>) and spaces show the hierarchy of the data structure.

Tip
Event ID is a system-assigned identifier for a specific electronic signature.

◆ See “Tables and Fields” on page 298.

Tip

In QAD Desktop, right-click the data frame and select Page Down and Page Up to scroll through the record.

See “Transaction Scoping” on page 320.

Note If the MFG/PRO data about to be displayed has never been signed, the system displays a message for the associated category.

You can scroll through the frame to view all the field values. Choose End to exit from the details frame and return to the program.

When you finish entering or updating data according to the standard menu program functionality, the system prompts you to enter an electronic signature.

Note The points at which a program saves updates to the database may change when electronic signatures are enabled.

The prompt screen includes the signature frame, as well as a details frame showing the data being signed. Figure 9.17 shows an example prompt from Labor Feedback by Work Order.

Fig. 9.17
Electronic
Signature Prompt

When Data Frame Optional is Yes for the active profile, initial focus is on the signature frame.

Displays only when Prompt for Preview E-Sig is Yes.

When Data Frame Optional is No for the active profile, initial focus is on the details frame.

Navigation in the details frame depends on the setting of Data Frame Optional in the active profile. When that field is No, focus is immediately on the details frame so you can scroll through the entire record. You must choose End to place focus on the signature frame. When Data Frame Optional is Yes, immediate focus is on the signature frame. However, you can still scroll the details by setting Scroll Details to Yes. When you finish reviewing the list of field values, choose End to return to the signature frame.

In menu programs that create transaction records, these signature frames may display before the transaction records are created, depending on the value of Prompt for Preview E-Sig in the activated profile. In this case, the user can choose to complete the signature based on the incomplete data displayed in the details frame by setting Show Final Data to No. The transaction records are created, and the signature is recorded along with values for all signed fields, including the transaction record fields.

▶ See “Prompt for Preview E-Sig” on page 310.

To see the final data to be signed including the transaction records, set Show Final Data to Yes. The system generates the transaction records and displays the signature and details frames.

To sign the data, you must enter your user ID, MFG/PRO password, and a valid reason code defined for reason type ESIG. Depending on the Prompt for Remarks field in the active profile, you may also be able to enter a remark related to the signature.

Tip
The User ID field must be the same as your MFG/PRO log-in ID.

If for some reason you choose not to sign or the signature is not accepted, the system rolls back the entire database transaction, including all user modifications.

Important Be careful to enter the same user ID you used for log-in, as well as the correct case-sensitive password. Based on settings in Security Control (36.3.24), too many invalid signature attempts can cause your session to terminate, deactivate your user ID, and inform the system administrator of a potential unauthorized access attempt.

▶ See “Review Security Control Settings” on page 303.

Depending on how security is set up in your system, the system may prompt you to change your password. For example, this can happen if the password has reached its expiration date while you were logged in, or if the system administrator has forced a password change for your user ID.

After signature processing is completed, the system displays a message indicating that the signature has been successfully executed, along with the event identifier. Figure 9.18 shows an example.



Electronic Signature Successfully Executed. Event ID: 200406070000608011

Fig. 9.18
Signature Completion Message

► See “Apply Profile to Menu Programs” on page 312.

Transaction Scoping

So that the system can apply electronic signatures to the appropriate data, transaction scoping—the points during program execution when data is committed to the database—has been modified in some maintenance and transaction programs that can be signature enabled.

For example, before electronic signature functionality was added, each frame in Inventory Control (3.24) was included in an individual transaction block. You could update the first frame, choose Go, then choose End from the second frame. The system updated the database with the changes to the first frame. You did not have to choose Go through all the frames.

However, all frames are now part of one transaction block—allowing the system to apply the same electronic signature to all updates made in the program. If you update the first frame, choose Go, and choose End in the second frame, the changes you made in the first frame are not saved to the database. You must choose Go through all the frames to save any changes you make in the program.

Product Change Control

If you use electronic signatures with the Product Change Control (PCC) module, Incorporation (1.9.7.5) and Implementation (1.9.7.13) do not behave the same way as other signature-enabled programs.

Because all product change orders (PCOs) that are available for incorporation or implementation are selected by the system and processed only once, no current signature record is ever available for display when one of these programs executes. Additionally, the programs do not display the records being signed. Instead, the system just prompts for an electronic signature for each PCO to be incorporated or implemented.

Each PCO is processed in one transaction. If an error occurs during incorporation or implementation processing, all data related to this PCO is rolled back—including updates to product structures, routings, and so on. Other PCOs processed in the same program session are not affected.

If the user presses End in the E-Signature frame, the system does not create an electronic signature, and rolls back the incorporation or implementation transaction for the PCO. It then continues to process the next PCO.

Note You cannot use batch processing with Incorporation or Implementation when electronic signatures are enabled for the program. The Batch ID field does not display.

E-Mail Notifications

The system generates and sends e-mails to the administrator group set up in Security Control (36.3.24) in the following situations:

- One or more signature profiles are activated.
- A user's consecutive number of failed electronic signature attempts exceeds the Max Access Failures value in Security Control.

▶ See "Review Security Control Settings" on page 303.

The e-mail text is defined in master comment data. You can customize this text for your environment by modifying the text using Master Comment Maintenance (25.12).

The electronic signature-specific messages have a comment type of ES. The comment reference varies depending on the specific purpose. The e-mail is constructed by starting with a specific comment, followed by one or more MFG/PRO messages with additional details. A generic comment of type AT with a reference of `email_postfix` is appended. This comment contains the following information that applies to all system-generated security and enhanced controls e-mails:

This email was automatically generated from an MFG/PRO process. If you have any questions about this E-mail, contact the MFG/PRO system administrator. Do not reply to this E-mail.

Signature Profile Activation E-Mail

Comment Reference: `email_esig_profile_activation`

Comment Type: ES

The e-mail sent for signature profile activation is similar to this example.

The purpose of this e-mail is to inform you that one or more e-signature categories has been activated. You have been included in this e-mail distribution because you belong to the Administrator group identified in User Security Control for MFG/PRO. The information listed below regarding the activation can be used to obtain a detailed report of the activation by running the Activated E-Sig Profile Report.

The activation was performed by User ID: XXX

The newly activated profiles are set to begin on date: dd/mm/yy

The number of newly e-signature enabled activated profiles: #

The number of newly e-signature disabled activated profiles: #

This email was automatically generated from an MFG/PRO process. If you have any questions about this E-mail, contact the MFG/PRO system administrator. Do not reply to this E-mail.

Signature Failure E-Mail

Comment Reference: email_failed_esig_prefix

Comment Type: ES

The e-mail sent to the administrator group when failed signature attempts exceed the Security Control value is similar to this example:

The purpose of this e-mail is to inform you a user has been deactivated for exceeding the maximum e-signature failures allowed as set up in Security Control. You have been included in this e-mail distribution because you belong to the Administrator group identified in Security Control for MFG/PRO.

User ID deactivated for exceeding max e-sig failures allowed: XXX

This email was automatically generated from an MFG/PRO process. If you have any questions about this email, contact the MFG/PRO system administrator. Do not reply to this email.

Reporting

Reports and inquiries related to electronic signatures are available in three areas:

- Setup
- Electronic signature reports
- Functional reporting for programs that are signature enabled

Setup Reports

The E-Signature Setup Menu has four reports that provide information on signature setup records:

- Use E-Sig Category Master Report (36.12.14.11) to view the top-table name and the filters available for categories.
- Use E-Signature Group Report (36.12.14.2) to view the categories assigned to each group.
- Use E-Sig Workbench Profile Report (36.12.14.6) to view the following kinds of information about the current workbench structure for a specified electronic signature category:
 - Settings that control processing and display of signatures in enabled programs
 - The list of programs that are signature enabled for the category
 - The list of field and tables that are included in the signature record
 - Optionally, information about filters associated with the category, if applicable

Note Depending on whether you have updated or refreshed a workbench profile since last activating it, this report does not necessarily show the settings currently in use for a category. Use Activated E-Sig Profile Report to view that information.

- Use Activated E-Sig Profile Report (36.12.14.9) to view information about profiles that have been activated using E-Signature Profile Activation. It displays the same types of information as E-Sig Workbench Profile Report, but lets you specify a range of categories over a range of effective dates.

Example To view all the profiles currently in use, leave the category code range blank and enter today's date in both date fields.

Note Although a date range is not required in the selection criteria, consider entering one. This significantly reduces the time required to generate the report.

Electronic Signature Reports

The Enhanced Controls Menu includes three reports that let you:

- Display signature events based on information related to the signature itself, such as the user, date, and meaning.
- Select database records based on ranges of values for fields in category top tables, and generate a report on related electronic signature history.
- Monitor log-in history records for failed electronic signature attempts.

Viewing Signature Events

Use E-Signature Events Report (36.12.4) to view data based on ranges of signature event IDs, user IDs, and dates when the signature was created. Optionally, you can limit the report to signatures related to a single specified category code.

The Summary/Detail field controls whether the report includes just basic information such as the user's name, date, and signature meaning, or also includes details of the signed data.

Fig. 9.19
E-Signature Events
Report (36.12.4)

The screenshot shows a software window titled "E-Signature Events Report" with a subtitle "All Domains (usd)". The window has a toolbar with icons for grid, print, save, delete, undo, redo, and help. Below the toolbar is a form with the following fields:

- Event ID: [text box]
- User ID: [text box]
- E-Sig Date: [text box] / [text box] / [text box]
- Category Code: [text box]
- Summary/Detail: [text box] (set to "Summary")
- To: [text box] (next to Event ID)
- To: [text box] (next to User ID)
- To: [text box] (next to E-Sig Date)
- Output: [text box]
- Batch ID: [text box]

Viewing Signature History

Use E-Signature History Report (36.12.5) to select database records and view historical electronic signature data associated with them. For example, you can report on the two latest signature events associated with a specified work order.

Fig. 9.20
E-Signature History
Report (36.12.5),
Initial Frame

This report includes multiple frames. First, specify the category, user ID range, and signature date range. Use the following fields to control other characteristics of the report:

Max Events. Specify the maximum number of electronic signature events to be included in the report for each selected record. The default is 1, which displays the latest signature event for each record that matches the data ranges in the E-Record Selection Criteria frame. If you enter a larger number, the system displays the latest first, then works backward through the number of events specified.

Display Only Current. Indicate whether the system should limit the selection to records in which no data has been updated since the latest electronic signature was recorded.

Display Where the Table Data Is Unsigned. Indicate whether the system should include records matching the criteria data ranges even if they are not covered by an electronic signature instance. When this is Yes, the output identifies records that do not have associated signatures.

Auto-Select All. Indicate if you want all the fields in the top table to be included in the report by default. You can modify the setting for individual fields as needed in the Report Display Fields frame. The default is Yes.

◆ See Figure 9.22 on page 327.

Press Go to display the E-Record Selection Criteria frame where you can identify the records for which you are interested in seeing signature histories. Specify ranges of values for one or more fields in the top table for the category.

Note Large reports may result if you do not specify field-level selection criteria.

Fig. 9.21
E-Signature History
Report, E-Record
Selection Criteria

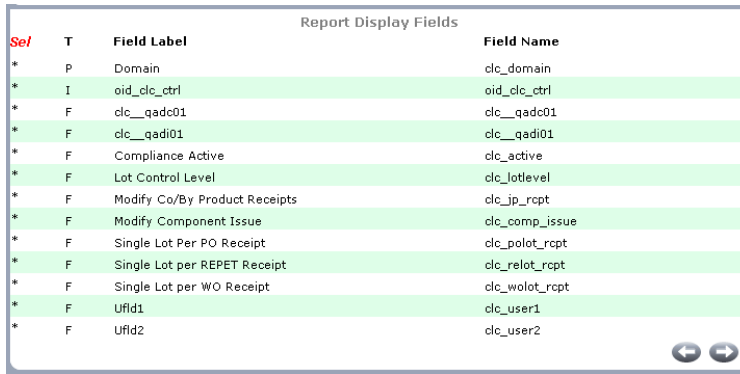
Table Name: clc_ctrl		Compliance Control	
E-Record Selection Criteria			
T	Field Label - Name	From Value	To Value
P	Domain - clc_domain		
I	oid_clc_ctrl - oid_clc_ctrl		
F	clc__qadc01 - clc__qadc01		
F	clc__qadi01 - clc__qadi01		
F	Compliance Active - clc_active		
F	Lot Control Lev - clc_lotlevel		
F	Modify Co/By Pro - clc_jp_rcpt		
F	Modify Compon - clc_comp_issue		
Data Range			
Field Name: clc_domain			
From Value:			
To Value:			

► See “Top Tables”
on page 299.

This frame displays the name, label, and type for each field in the top table of the selected category. Field types are Primary (P), Indexed (I), or non-indexed (F). Any selection criteria entered in the Data Range frame display next to the corresponding field on the E-Record Selection Criteria frame. These selection criteria are used to narrow the search results.

To minimize the report output, enter criteria for as many table fields as needed. For example, if you are reporting signature records for the Quality Results category (0002), you can limit the report to signatures for a specific work order. Scroll to the Work Order (wr_nbr) field and press Go. Enter the work order number in both the From Value and To Value fields. After entering the field-specific selection criteria for your report, choose End to continue.

Use the Report Display Fields frame to select or deselect the top-table fields to include or exclude on the resulting output.



Sel	T	Field Label	Field Name
*	P	Domain	clc_domain
*	I	oid_clc_ctrl	oid_clc_ctrl
*	F	clc_qadc01	clc_qadc01
*	F	clc_qadi01	clc_qadi01
*	F	Compliance Active	clc_active
*	F	Lot Control Level	clc_lotlevel
*	F	Modify Co/By Product Receipts	clc_ip_rcpt
*	F	Modify Component Issue	clc_comp_issue
*	F	Single Lot Per PO Receipt	clc_polot_rcpt
*	F	Single Lot per REPET Receipt	clc_relot_rcpt
*	F	Single Lot per WO Receipt	clc_wolot_rcpt
*	F	Ufid1	clc_user1
*	F	Ufid2	clc_user2

Fig. 9.22
E-Signature History
Report, Report
Display Fields

All fields are preselected if Auto-Select All is Yes in the first frame. Select or deselect fields as needed. Then press Go to specify the output device for the report.

The report output includes the values for all the top-table fields selected in the Report Display Fields frame, as well the following signature data for each event:

- Event ID
- User ID and name of the person signing
- Name of the MFG/PRO menu program that generated the signature
- Signature meaning—the reason code entered when the record was signed
- Signature date and time
- Remark entered with the signature
- Current indicator, specifying whether signature values and database values are still identical
- Signed data—the value when signed of each field included in the active profile in effect when the signature was created

Note If signature events are not available that match the selection criteria, the output includes the following message:

Data archived or never signed

The latest signature should always be available. It is not deleted during an archive/delete.

Monitoring Failed Signature Attempts

As part of an overall security program, you can generate a report showing unsuccessful signature attempts, based on user log-in history records.

Use E-Signature Failure Report (36.12.7) to select history records by a combination of user ID, signature attempt date, and status code. The resulting report displays the user ID and name, time data, and the status code, which identifies the reason for failure; for example, ID deactivated because of excessive failed signature attempts.

When failed log-in history records are no longer needed online, you can remove them using E-Sig Failure Archive/Delete (36.12.14.21). This standard archive/delete program deletes records from the system and optionally saves them to a file.

Functional Reports and Inquiries

Some reports and inquiries associated with signature-enabled menu programs let you include electronic signature data in the output. When Display E-Signature Details is Yes, the system displays information about the signature such as the individual who signed the record, as well as values of the signed data fields.

Note The display of this field is conditional. It only appears on the user interface when both the following are true in the active profile for the appropriate category:

- ◆ See page 307.
- ◆ See page 312.
- E-Signature On is set to Yes.
- The menu program has Apply selected.

Based on those values, the reports and inquiries listed in Table 9.6 can include the Display E-Signature Details field.

Table 9.6
Reports and
Inquiries
Displaying
Electronic
Signature Data

Program	Menu	Category
PCR/PCO Detail Inquiry	1.9.2.8	0010
Print PCR/PCO	1.9.9.1	0009
Lot Master Inquiry	1.22.2	0005
Inventory Detail by Lot Inquiry	3.1.13	0006
Inventory Detail by Item Inquiry	3.2	0006

Program	Menu	Category
Inventory Detail by Site Inquiry	3.3	0006
Inventory Detail Report	3.6.5	0006
Inventory Detail by Location Report	3.6.6	0006
Inventory Detail Report	3.6.5	0006
Transactions Detail Inquiry	3.21.1	0007
Operation Transaction Detail Inquiry	17.9	0003
Operations by Work Order Report	17.14	0003
Operations By Employee Report	17.15	0003
Quality Order Results Report	19.12	0008
Certificate of Analysis Print	19.20	0008
Control Table Report	36.17.6	0001 or 0004 ¹

1. The signature details field displays in Control Table Report if the profile conditions are met for either category.

Important In some inquiries, if Output is set to a display device such as Terminal rather than to a printer or a file, electronic signature data is not included regardless of this setting. Change the output device to view that data. This limitation does not apply to reports.

Archiving and Restoring Records

Use E-Signature Archive/Delete (36.12.14.22) to archive and optionally delete electronic signature records from the system when they are no longer needed online.

If you need to access the records later, you can reload them using E-Signature Restore (36.12.14.23) based on ranges of signature dates and category codes. They are then available to E-Signature Report.

Tip
You cannot delete signature records without archiving them.

Fig. 9.23
E-Signature
Archive/Delete
(36.12.14.22)

Select records by entering the last electronic signature creation date you want the system to consider. The system selects all records up to that date that have not previously been archived.

Note To ensure that signature-enabled programs can always display the latest signature data, the system does not delete the record for the latest signature event. It archives these records if they meet the selection criteria, but does not delete them even when Delete is Yes. The records are automatically deleted during a subsequent archive/delete session if they no longer represent the latest signature.

Because electronic signatures are typically associated with a high-security environment that emphasizes user accountability, this function is unlike other MFG/PRO archive/delete programs. In those programs, records are archived to a data file for storage outside the database. However, E-Signature Archive/Delete instead creates records in the same audit databases used by the audit trail functions of the Enhanced Controls module.

► See “Set Up Audit Trails” on page 302.

Important So that they can be tracked properly for recovery, records are stored based on the signature event dates. This means that audit databases with connection records in Audit DB Maintenance (36.12.13.11) that have E-Signature set to Yes and that cover the correct date ranges must be running when archiving takes place so that the system can connect to them as needed. The same audit databases must be available when you restore the records.

Fig. 9.24
E-Signature
Restore
(36.12.14.23)

The screenshot shows a software dialog box titled "E-Signature Restore" with a subtitle "All Domains (usd)". Inside the dialog, there are four input fields: "From Date:" (with a calendar icon), "Category Code:", "To:" (with a calendar icon), and another "To:" field. Below these fields is a label "Records:". At the bottom right, there are two circular navigation buttons, one with a left arrow and one with a right arrow.

Glossary

Application Program Interface (API). A set of routines, protocols, and tools that connect applications, usually for the purpose of sharing data.

Audit Profile. A record associated with a specific database table that contains information that controls the table auditing, including a detailed list of fields and field types in the table, a logical field that determines whether auditing is enabled, and a list of delete event keys associated with the table.

Connection Domain. A domain associated with a connected database, not the current working database.

Consolidation Domain. Refers to the domain where consolidation takes place. This can be a domain set up specifically for this purpose only, but this does not have to be the case. You can use a domain that represents an active business operation in the database

Consolidation Set. A way of identifying the group of subsidiary entities with GL transactions that need to be reported by a parent entity. The system uses attributes of the consolidation set to manage the GL consolidation process.

Default Domain. The domain a user typically works in. Each user is assigned a default domain that displays during log-in.

Delete Event Key. Fields used to identify deleted records in the audit database. Initially, the primary index fields for each database table are defined as delete event keys. Users can add additional keys as needed.

Destination List. A list of application IDs registered with Q/LinQ that can be used for publishing, sending, and deleting or archiving documents. Destination lists create only one copy of a document for management and storage, minimizing disk space and performance requirements.

Domain. A business operation with a single currency and chart of accounts. Each database must have at least one domain and can have as many as required. Each domain can include one or more entities, one of which is designated as primary.

Electronic Signature Category. A QAD-provided definition of a set of MFG/PRO data that can be signed as a unit in certain menu programs.

Electronic Signature Profile. A record that contains information that controls how electronic signatures are applied for a given signature category. It includes list of programs that create signatures, a detailed list of tables and fields included in the signed record, filters that determine whether specific records are subject to signatures, and fields that control various aspects of the signature process.

Extensible Markup Language (XML). A specification designed especially for Web documents that allows the definition, transmission, validation, and interpretation of data between applications and organizations.

Filter Criteria. A conditional clause in a synchronization profile that determines which records from a table to synchronize.

Object ID (OID). A means of uniquely identifying a database record. In MFG/PRO, OIDs are decimal values based on a date/time stamp and sequence number on the left of the decimal. The right side of the decimal is a registration value based on the OID Generator Code specified in Database Control (36.24).

Payload. The data fields specified in a synchronization profile whose values are included in a synchronization document.

Primary Domain. A domain associated with the current database.

QDoc. A data document in XML format inbound to MFG/PRO that conforms to generated schemas and events files from the QGen utility.

Schema Trigger. Progress .p procedures added through the Data Dictionary to the database schema. Schema triggers always execute when a specified event occurs.

Simple Object Access Protocol (SOAP). A protocol for exchanging information in a decentralized, distributed environment in XML format.

Synchronization Document. A document representing a single add, change, or delete action for a specific master table record.

Synchronization Profile. Specifies which data to synchronize (tables, fields) and which data changes to synchronize (add, change, delete).

System Domain. A special domain containing default data that is created during database initialization and used as a template when creating new domains. System domains are identified with a type of SYSTEM.

XML. See *Extensible Markup Language (XML)*.

Index

Symbols

! (exclamation point) 239
* (asterisk) 239
~REPORTS 61
~SCREENS 61

Numerics

1.1.13 65
2.14.1 225
3.21.19 82
17.13.22 82
18.4.16 82
18.22.4.12 82
25.3.1.1 100
25.3.4 95
25.13.7 95
25.19.1 95
25.19.4 105
25.19.10 105
25.19.11 105
25.19.13 109
25.19.14 95
25.19.15 95
25.19.17 95
25.19.20 107
25.3.1.7 115
26.1 74
26.4 74
26.7 74
26.10 75
26.12 76
35.11.1 174
35.11.11 174
36.3.1 68, 223, 240
36.3.4 233, 235, 243, 245
36.3.6 243
36.3.7 245
36.3.8 248

36.3.11 249
36.3.12 250
36.3.16 246
36.3.21.1 70
36.3.22 234
36.3.23.1 198
36.3.23.12 230
36.3.24 213
36.5.3.24 238
36.6.1 58
36.8.1.1 122, 144
36.8.1.2 152, 163
36.8.1.3 152
36.8.1.4 160
36.8.1.5 162
36.8.1.20 149
36.8.5 170
36.8.7 166
36.8.8 151
36.8.9 166
36.8.10 167
36.8.11 168
36.8.13 168
36.8.14 168
36.8.16 168
36.8.17 168
36.8.18 169
36.8.22.1 133
36.8.22.2 133
36.8.22.3 132
36.8.22.4 132
36.8.22.8 164
36.8.23 170
36.8.24 143, 146
36.10.1 59
36.10.3 63
36.12.1 282
36.12.2 282

- 36.12.4 324
- 36.12.5 324
- 36.12.7 328
- 36.12.13.1 271
- 36.12.13.2 272
- 36.12.13.4 272
- 36.12.13.5 275
- 36.12.13.6 277
- 36.12.13.8 277, 315
- 36.12.13.9 278
- 36.12.13.11 263
- 36.12.13.23 278
- 36.12.13.24 279
- 36.12.14.1 305
- 36.12.14.4 306
- 36.12.14.5 308
- 36.12.14.9 316
- 36.12.14.21 328
- 36.12.14.22 329
- 36.12.14.23 329
- 36.14.3 83
- 36.14.4 84
- 36.14.5 84
- 36.14.13 84
- 36.16.10.1 234
- 36.18.24 69
- 36.20.10.15 72
- 36.24 67, 260

A

- Access Code/Path field 147
- accounts
 - cross-referencing 105
 - currency 74
- action types 122
- Activated Audit Profile Report 278
- Activated E-Signature Profile Report 316
- active domain 61
- active reason code 229
- active status of user 229
- adapter program 147
- add data actions 122
- address, e-mail specification 227
- addresses, setting up profiles 138
 - customer ship-to 139
 - customers 139
 - list type 140
 - supplier 139
 - supplier remit-to 140
- administrator group
 - auditing e-mail 261
 - security e-mail 222

- All Domains display 70
 - programs 185
- API type, User Maintenance 226
- application IDs 144
- application program interfaces (APIs)
 - exchanging documents 165
 - messaging API 147
 - stream API 147
- applications, assigning in User Maintenance 225, 234
- AR Self-Billing 44
- archive/delete
 - consolidation entities 115
 - e-sig failures 328
 - e-signatures 329
 - Q/LinQ documents 170
- assigning applications in User Maintenance 225
- audit databases 257
 - archiving electronic signatures 302, 330
 - online 265
 - Oracle environments 268
- Audit DB Maintenance 263
- Audit Group Maintenance 271
- Audit Group Report 272
- Audit Profile Activation 277
- audit profiles
 - activating 277
 - definition of 254
 - delete event keys 276
 - groups 271, 305
 - overview 270, 304
 - refreshing 272
 - updating in workbench 275
- Audit Trail Control 279
- Audit Trail Creation Process 257, 278
- Audit Trail Report–Deleted 282
- Audit Trail Report–Existing 282
- Audit Trails
 - Audit DB Maintenance 263
 - audit profiles 254
 - Audit Trail Creation Process 278
 - data flow 257
 - delete event keys 254
 - overview 33
 - planning audit system 261
- Audit Workbench Profile Maintenance 275
- Audit Workbench Profile Report 277
- Audit Workbench Refresh 272
- auditing
 - data flow 257
 - delete event keys 254, 276
 - overview 33, 35
 - planning 261

reports 282
 setup workflow 254

B

Bank Maintenance
 entity 98
 batch processes, user ID requirements 224
 Batch Request Browse 84
 Batch Request Detail Maintenance 83
 Batch Request Detail Report 84
 Batch Request Processor 84
 batch requests
 managing 83
 bill of material, profile for 140

C

categories, electronic signature 295
 Change Current Domain 63
 Change Current ECommerce Domain 174
 change data actions 122
 changing domains 63
 EDI ECommerce processing 178
 character-based menu 228
 checklists, security implementation 210
 CIM
 debugging 168
 delete 125
 format 125
 processing 158
 Code Mapping Maintenance 149
 committing data to database 320
 communication
 caller, listener processes 148, 165
 error recovery 170
 messaging API 147
 stream API 147
 compiles, protecting in Progress 204
 connection records
 database 58
 domains 60
 consolidation entity 98
 Consolidation Entity Delete/Archive 115
 consolidation sets 97
 consolidation, general ledger
 See GL consolidation
 control programs
 Audit Trail 279
 database 67
 Q/LinQ 146
 security 69, 213
 control tags 156
 conversion

audit trails 35
 domain 16
 EDI ECommerce 27
 Intrastat 48
 security 32
 country
 information in locale.dat file 226
 setting country code for user 225
 Country Code Maintenance 225
 County Code field 225
 cross-references
 accounts 105
 EDI ECommerce processing domains 177
 Ctrl+F display 71, 216
 currencies
 calculating exchange rates 76
 exchange rate relationships 75
 exchange rates 74
 setting up 73
 translation of 108
 Currency Account Maintenance 74
 Currency Maintenance 74
 Current field 317
 customer addresses, profiles for 139
 customer ship-to address, profiles for 139
 Customer type, User Maintenance 226

D

data
 capture 118
 committing to database 320
 control tags 156
 documents created 122
 flow 119
 identification key 122
 mapping 125
 overview 118
 profiles for 132
 setting up 130
 to synchronize 126
 data dictionary
 field security 243
 data mapping procedures 158
 Database Connection Maintenance 58, 263
 Database Control 67
 OID Generator Code 260
 database tables
 non-domained 182
 databases
 access control 204
 audit connection parameters 263
 auditing 257

- caller, listener processes 148
 - communication errors 170
 - connection records 58
 - conversion for domains 16
 - events 118
 - multiple
 - auditing data flow 262
 - auditing requirements 260
 - Progress security 203
 - registering with Q/LinQ 144
 - sequences 18
 - switching 64
 - synchronization flow 119
 - triggers 18
 - DBAUTHKEY function in Progress 204
 - Debug CIM Document 168
 - default domain 232
 - delete data actions 122
 - delete event keys 276
 - definition 254
 - delete/archive
 - consolidation entities 115
 - e-sig failures 328
 - e-signatures 329
 - Q/LinQ documents 170
 - using with domains 18
 - Derived Exchange Rate Calculation 76
 - Desktop
 - log-in domain 201
 - security 197
 - using with Domains 84
 - Destination List Maintenance 151
 - destination lists
 - communication error recovery 171
 - defined 150
 - deleting logs 170
 - log files 168
 - tracking 170
 - destination MFG/PRO procedures 158
 - Dictionary Field Security Report 242, 243
 - direct allocation, EMT 80
 - Distribution Requirements Planning (DRP)
 - domains 81
 - documents
 - correcting, reprocessing 168
 - deleting 170
 - export specifications 152
 - exporting 165
 - import specifications 152
 - importing 165
 - mapping 167
 - processing 167
 - publishing enabled 155
 - publishing, automatic and manual 163
 - standards, types 155, 157
 - tracking 168
 - triplet format 122
 - Domain Cross-Reference Maintenance 174, 177
 - Domain Maintenance 59
 - domains
 - application IDs for 144
 - batch requests 83
 - changing 63
 - connection records 60
 - conversion required 16
 - creating 59
 - cross-domain features 82
 - cross-domain functions 185
 - default 232
 - multi-database environment 60
 - overview of changes 10
 - security access 201
 - setting up 56
 - specifying in Q/LinQ 147
 - subsidiary 102
 - synchronization relationships 120
 - synchronizing data 120
 - system 59
 - user access to 68
 - user groups and 233
 - using Q/LinQ with 117
 - Dump Export/Import Doc for Edit 168
 - Dump Export/Import Docs to File 169
 - Dynamics Site Number 259
- E**
- ECommerce Function Maintenance 179
 - ECommerce. *See* EDI ECommerce
 - EDI ECommerce 173–180
 - multi-domain processing 174
 - summary of changes 25
 - transformation definitions 178
 - electronic signature categories 295
 - electronic signature profiles
 - activating 315
 - refreshing 306
 - updating in workbench 308
 - Electronic Signatures 290–330
 - e-mail
 - auditing notifications 280, 321
 - electronic signature notifications 303
 - notification settings 146, 155, 158, 217
 - security notifications 222
 - user's address 227

employee type, User Maintenance 226
 Enforce Licensed User Count 214, 225
 Enhanced Controls 254–330
 Enterprise Material Transfer (EMT)
 direct allocation 80
 with domains 79
 Enterprise Operations Planning (EOP)
 domains 82
 entities
 consolidation 98
 delete/archive consolidation 115
 security 247
 setting up 97
 Entity Code Maintenance 100
 Entity Consolidation Detail Inquiry 105
 Entity Consolidation Detail Report 105
 Entity Security Maintenance 248
 error recovery 170
 errors, license violations in User Maintenance 215
 E-Sig Failure Archive/Delete 328
 E-Signature Archive/Delete 329
 E-Signature Events Report 324
 E-Signature Failure Report 328
 E-Signature Group Maintenance 305
 E-Signature History Report 324
 E-Signature Profile Activation 315
 E-Signature Restore 329
 E-Signature Workbench Profile Maintenance 308
 E-Signature Workbench Refresh 306
 Exchange Rate Maintenance 74
 Exchange Rate Relationship Maintenance 75
 exchange rates
 calculating derived 76
 defining 74
 GL translation 95
 relationships between 75
 Export Specification Maintenance 152, 163
 Export/Import Doc Delete/Archive 170
 Export/Import Document Query 168
 Export/Import Document Report 168
 Export/Import Spec Copy 160
 Export/Import Specification List 162
 exporting
 communication errors 170
 document specifications 152
 document standards, types 155
 documents 165
F
 field security 242
 validation 243
 Field Security by Group 245

Field Security Maintenance 243, 245
 file transfer 166
 filters, electronic signature 300, 311, 314
 Fixed Assets
 reporting 43
 Force Password Change Utility 230
 Foreign Exchange Revaluation 109
 From-Account Cross-Reference Maintenance 105,
 108

G

general ledger (GL)
 account security 248
 enhancements 42
 General Ledger Control
 translation adjustment accounts 108
 GL Account Security Maintenance 248
 GL Calendar Maintenance 95, 109
 GL Consolidation 107
 account cross-references 106
 correcting transactions 108
 processing 107
 reprocessing 110
 summary of changes 19
 GL consolidation
 consolidation sets 97
 cross-reference accounts 105
 in a single database 96
 multiple database work flow 94
 overview 90
 preparing for 93
 steps afterwards 109
 Global Tax Management (GTM)
 reporting 40
 gppswd.v 243
 groups
 auditing 271, 305
 electronic signature 305
 user 234
 GRS Control 45

H

Header Display Mode setting 59, 69, 215
 host name 147

I

Import Specification Maint 152
 Imported Transaction Revaluation 95, 109
 importing
 communication errors 170
 document specifications 152
 document standards, types 157

- documents 165
- Inquiry by Account with Drill-Down 111
- interface preferences 228
- Interface Session Monitor 170
- International Organization for Standardization (ISO)
 - codes 225
- Intrastat 45
- Inventory Movement Code Security 249
- Inventory Movement Code Security Browse 250
- Invoice Post
 - site security 246

L

- Language field, User Maintenance 225
- languages
 - identifying for users 225
- License Registration 234
- licenses
 - tracking violations 215
- licensing
 - interaction with User Maintenance 224
 - warnings versus errors 215
- locale.dat file 226
- log files
 - auditing 279
 - deleting information 170
 - destination lists 168
- log-in
 - security 198
 - using operating system user ID 200
- Logon Attempt Report 198

M

- mapping
 - documents 167
 - procedures 158
- material requirements planning (MRP)
 - site security 246
- menu security 240
- Menu Security Maintenance 142, 240
- menu styles, User Maintenance 228
- menu substitution, User Maintenance 228
- menus
 - character-based 228
 - security 240
 - security for Windows icons 241
 - setting up styles for users 228
 - tear-off style 228
- messaging API 147, 165
- Multi Domain field 70
- multiple databases
 - distribution requirements planning (DRP) 81

- domains in 60
- enterprise material transfer (EMT) 79
- enterprise operations planning (EOP) 82
 - GL consolidation work flow 94
- sites 65
- multiple languages 18

N

- named user license 224

O

- object ID (OID) 17
- operating system
 - security 201
 - using ID for MFG/PRO log-in 200
- Operation Transaction Numbering Report 82
- Oracle, audit database 268

P

- parameter file
 - audit database connection 267
- passwords
 - creation method 221
 - forcing change 230
 - managing 197
 - Security Control settings 219
 - updating 230
- payload, synchronization profile 118
 - updating 136
- PO Reference Date Logic field 45
- ports 147
- Primary location for user access 230
- Process Import Documents 167
- processing
 - CIM 158
 - documents 167
 - programs 158
- Product Change Control (PCC)
 - enhanced features 39
 - using electronic signatures with 320
- product structure, profile for 141
- profiles. *See* synchronization profiles
- Program Information Maintenance 70
- Progress 204
 - blank user ID 203
 - compiles, protecting 204
 - database access 204
 - DBAUTHKEY function 204
 - editor security 202, 242
 - passwords 204
 - RCODEKEY function 204
 - schema controls 203

Progress Application Server
 multithreaded MRP and DRP 50
 Progress Corporation
 Dynamics Site Number 259
 protection. *See* security
 publishing documents
 automatic and manual 156, 163
 enabling 155
 table updates 156
 Purchasing 44

Q

Q/LinQ 117–171
 administration 167
 destination lists 150
 document specifications 152
 processing documents 167
 publishing documents 163
 registering applications 144
 summary of changes 21
 synchronization profiles 132
 synchronizing data 118
 system IDs 143
 Q/LinQ Control
 e-mail notification settings 146
 system ID 143
 QAD Desktop
 log-in domain 201
 using with domains 84
 QAD type, User Maintenance 226
 QDocs
 overview 22
 qqqq2qq.p 147
 QXtend Inbound
 overview 22

R

RCODEKEY function in Progress 204
 reason codes
 active reason 218, 229
 electronic signatures 302
 Receive Import Documents 166
 record-locking during signature entry 310
 records, identifying 122
 recovery, communication errors 170
 Register External Application 122, 144
 registered applications, assigning to users 225
 Reload Edited Export/Import Doc 168
 reports
 audit data 282
 electronic signatures 324
 restarting sessions 171

restricting access. *See* security
 routings, profile for 142

S

Sales and Use Tax Interface (SUTI)
 controlling access 238
 enhancements 42
 schema, controlling in Progress 203
 security 193–251
 Dictionary Field Security Report 242
 domain 201
 entity 247
 field 242
 field limitations 243
 for Q/LinQ programs 142
 GL accounts 248
 implementation checklists 210
 inventory movement code 249
 log-in 198
 menu 240
 monitoring 250
 operating system 201
 overview 195
 password management 197
 planning 208
 Progress editor 202, 242
 Progress level 204
 schema level 203
 site 246
 special characters 240
 types of 196
 wild cards 238
 Windows systems 206
 workstation 205
 Security Control 59, 213
 administrator group 261
 Header Display Mode field 69
 Send Export Documents 166
 sequence numbers
 database 82
 sequences 18
 server time zone 67
 Server Time Zone Change Utility 68
 Service Management Control 68
 Service/Support Management (SSM)
 enhancements 48
 Session ID Prefix field 214
 Session Master Maintenance
 domain 72
 sessions
 restarting 171
 tracking 170

- signature meaning 302
- Site Maintenance
 - associating domain 65
 - entity 98
- site security 246
 - excluded functions 246
 - ranges of sites 247
 - setting up 247
- Site Security Maintenance 246
- sites
 - domain associated with 65
- SO Reference Date Logic field 45
- SOAP 22
- sockets 147
- Standard Transaction Maintenance 109
- stream API 147, 165
- summarized transactions 102
- supplier addresses, profile for 139
- supplier remit-to address, profiles for 140
- switching databases 64
- switching domains 63
- Sync Table–Field Browse 132
- Sync Table–Field Maintenance 132
- synchronization 118, 122, 130, 132
- Synchronization Mass Export 164
- Synchronization Profile Inquiry 133
- Synchronization Profile Maintenance 133
- synchronization profiles
 - addresses 138
 - BOM code 140
 - define 132
 - general setup 133
 - header-detail tables 137
 - product structure 141
 - routings 142
 - selection criteria 133
- synchronization relationship types 120, 121, 144
- System Access frame, User Maintenance 229
- system domain 59
 - data loaded into 188
- system ID, Q/LinQ 143

T

- tables
 - without Domain field 182
- Tax Interface Control 238
- TCP/IP 147
- text files, document exchange 166
- time zone
 - server 67
 - setting up in User Maintenance 227
- Timeout Minutes field 205, 214

- top tables, electronic signature 299
- tracking
 - documents 168
 - log-in attempts 250
 - sessions 170
- Trading Partner Library Load 179
- Transaction Export 95
- transaction history, viewing 82
- Transaction Import 95
 - account cross-references 106
- Transaction Numbering Report 82
- Transaction Post 95, 97
- transaction scoping 320
- transactions
 - correcting XC 108
 - GL, importing and exporting 94
 - GL, summarized 102
- Transformation Definition Maintenance
 - changing domains 178
- Translation Adjustment Account (BS) 108
- Translation Adjustment Account (IS) 108
- Translation Exchange Rate Maintenance 95, 97, 108
- triggers, schema replication
 - domain effect 18
 - overview 118
- triplet format 122
- type
 - domain 62
 - entity 100
 - user 226

U

- update types 122
- User Access by Application Inquiry 234
- User Group Maintenance 233, 235
- user groups 234
- user ID
 - at log-in 198
 - blank, in Progress 203
 - deleting 224
 - displaying at user interface 216
 - Progress 204
 - setting up 223
- user interface
 - Desktop 84
 - domain effect 69, 215
- User Maintenance 68
 - country code 225
 - interface preferences 228
 - language 225
 - locale 225
 - time zone 227

- user groups 233
- user type 226
- variant 225
- violation messages for license agreement 224
- user name
 - viewing 216
- User Type field 226
- user-defined functions, EDI ECommerce 179
- users
 - access to domains 68
 - assigning applications 225
 - defining types in User Maintenance 226
 - e-mail address 227
 - enforcing license agreement 225
 - groups 233
 - interface preferences 228
 - locale 225
 - menu styles 228
 - time zone 227
 - type 226
 - violation messages for license agreement 224

V

- Variant field, User Maintenance 225
- violation messages, licensing 224

W

- warning messages, license violations 215
- wildcards
 - use with security 239
- Windows security options 206
- work flow
 - auditing setup 254
 - currency setup 73
 - domain setup 57
 - electronic signatures setup 292
 - GL consolidation 96
 - GL transaction import/export 94
 - security setup 208
 - synchronization processing 162
 - synchronization setup 130
- workstation
 - security 207

X

- XC transactions 108
- XD document type 112
- XML 22
- XS document type 112

