



QAD Enterprise Applications
Enterprise Edition

Administration Guide Security

Introduction to Security
Security Overview
QAD .NET UI Security
Security Control
Authentication
Users and Roles
Channel Islands UI Security
QAD .NET UI Security
Segregation of Duties
E-signatures
Auditing
Reverse Proxy for Channel Islands

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.

This document contains trademarks owned by QAD Inc. and other companies.

Copyright ©2018 by QAD Inc.

Security_AG_v2017EE.pdf/sti/b3s

QAD Inc.

100 Innovation Place
Santa Barbara, California 93108
Phone (805) 566-6000
<http://www.qad.com>

Contents

Security Admin Guide Change Summary	ix
--	-----------

Chapter 1	Introduction to Security	1
------------------	---------------------------------	----------

Overview	2
User and Role-Based Security Model	3
System Security	4
System Security Features	4
Progress OpenEdge Security Configuration	5
Internal Controls	5
Implementation Summary	6
Establishing a Security Plan	6
Implementing Your Security Plan	7
Security Planning Checklists	7
Security and Internal Controls Programs	9

Chapter 2	Security Overview	13
------------------	--------------------------	-----------

Role-Based Access Security	14
Roles	14
Role Permissions	14
Role Membership	15
Additional Types of Security	16
Password Management	16
Sign-in Security	17
Workspace Security	17
Sign In and Security Control	18
OS-Based Sign-in Security	20
Operating System and Progress Security	20
Progress Editor Access	21
Progress-Level Database Schema Controls	22
Compiling Custom Code on Unprotected Databases	22
Client-Level Security	22
Windows Systems	23
Non-Windows Systems	23
QAD .NET UI Security	23

Chapter 3 Security Control 25

Define General Security Settings	26
Create a Password Strategy	30
Set Up E-mail Notifications	32
Monitor System Security	33

Chapter 4 Authentication 35

Overview	36
User Authentication	36
LDAP Authentication	36
Internal	36
Directory Services Markup Language Service	36
Configure Java Keystore	37
Install DSML Gateway	37
Review and Update Directory to QAD Database Mappings	39
Download QAD .NET UI	42
Configure SYNC reason code	42
Configure Alternate Country Code	42
Configure LDAP Instance	43
Verify LDAP Instance Definition for DSML Gateway Using User Sync	43
Test LDAP	45
API Authentication	46

Chapter 5 Users and Roles 47

Overview	48
Role and User Definition Process Workflow	48
Set Up Users	49
User Synchronization	50
Types of Users	50
Define Users	51
Specify Access to Domains and Entities	59
Set Up Roles	61
Uses of Roles	61
Define Roles	66
Define Role Permissions	67
Define Role Membership	70
View Access Information	71
Export and Import Roles and Permissions	72

Chapter 6 Channel Islands UI Security 73

Overview	74
Prerequisites	74

User and Role Workflow in Channel Islands	74
Resources	74
Channel Islands Resources	74
Users and Roles	75
Default Roles	75
Menus	76
Role Menu	76
Favorites Menu	79
Role Permissions	80
Permissions Inheritance and Configuration	82
Resource Dependencies	86
Role Permissions Actions	88
Assigning Permissions to Roles	89
Role Menu Dependency	93
User Access	95
Set System Access	95
Assign Roles	96
Configure Stored Views Access	97
Chapter 7 QAD .NET UI Security	99
SSH on the QAD .NET UI	100
Public Key Authentication for SSH	101
SSH for QAD .NET UI Terminal Mode	103
SSL on QAD .NET UI Tomcat Home Server	103
HTTPS for QAD .NET UI Desktop Screen Display	106
HTTPS for AIA	107
Additional Security for Standard Programs	107
Specifying User IDs and Roles	108
Limiting Access to Fields	109
Controlling Inventory Updates	112
Defining GL Account Security	123
Defining Inventory Movement Code Security	124
Chapter 8 Segregation of Duties	125
Overview	127
Segregation of Duties Verification	128
Segregation of Duties Compatibility Matrix	129
Segregation of Duties Policy Exceptions	129
Segregation of Duties Process Workflow	129
Plan a Segregation of Duties System	131
Segregation of Duties Rule Checking	132
Role Permissions Validation	132

Role Membership Validation	133
Direct and Indirect Violations	134
Segregation of Duties Rule Matrix	135
Complete Prerequisite Activity	138
Disable the Superuser Role	138
Activate Segregation of Duties	138
Activate Segregation of Duties from the Command Line	140
Maintain Segregation of Duties Categories	140
Delete Categories	141
SOD Category Excel Integration	141
Assign Resources to Segregation of Duties Categories	142
SOD Category Membership Excel Integration	144
Maintain the Segregation of Duties Matrix	144
SOD Matrix Excel Integration	147
Define Role Permissions	148
Define Role Membership	148
Maintain Segregation of Duties Policy Exceptions	149
Delete Policy Exceptions	150
Segregation of Duties Role Exclusions	150
Import and Export Segregation of Duties Data	151
SOD Category Worksheet	152
SOD Matrix Worksheet	152
Resource Worksheet	153
Role Worksheet	153
Export to Excel	154
Import from Excel	155
Export to XML	157
Import from XML	158
Report and View Logs and Violations	158
View Log History	158
Report on Current Segregation of Duties Conflicts	159
View Role Permissions Violations	161
Archive Log Record Files	162
Chapter 9 E-signatures	163
Overview	164
E-signature Enabled Programs	164
Programs for E-Signature Setup and Reporting	166
E-Signature Planning Steps	166
E-Signature Workflow	167
Set Up E-Signature Functionality	169
Load E-signature Initial Data	169
Set Up E-signature Reason Codes	169

Define Security Control Settings	170
E-Signature Categories	170
Category Considerations	173
Tables and Fields	173
Filters	175
E-Signature Profiles	176
Overview	176
Define E-Signature Profiles	177
Create Signature Groups	178
Refresh Signature Profiles	178
Update Signature Profiles	179
Activate E-signature Profiles	184
Record E-Signatures	185
Transaction Scoping	186
Product Change Control	187
E-Mail Notifications	187
Signature Profile Activation E-Mail	187
Signature Failure E-Mail	188
Reporting	188
Setup Reports	188
E-signature Records for Quality Control	189
E-signature Reports	189
Functional Reports and Inquiries	192
Archive and Restore Records	193
Chapter 10 Auditing	195
Overview	196
Plan Auditing	197
Determine Databases to Audit	197
Determine Tables to Audit	198
Archive Database Considerations	198
Auditing Custom Table Considerations	198
Set Up Auditing	198
Enable Auditing for the Database	199
Configure Database Options and Audit Permissions	199
Import Audit Policy	201
Enable Auditing on Selected Tables	202
Enable Auditing on Selected Fields	203
Generate Reports for Audit Configuration	204
Archive Database	204
Manage the Archive Database Server	205
Database Connection Report	206
Execute Archive/Load Scripts	207

Generate Audit Trail Reports	208
Generate Reports Against Application Databases	208
Generate Reports from Archive Databases	209
Export Audit Policy	210
Disable Auditing	211
Chapter 11 Reverse Proxy for Channel Islands	213
Overview	214
Configuration	214
Proxy Configuration	214
URL Rewriting	214
Configuring Caching of Java Objects	217
Disk Store Configuration	218
Refresh Ahead Caching	218
Product Information Resources	221
Index.....	223

Security Admin Guide Change Summary

The following table summarizes significant differences between this document and previous versions.

Date/Version	Description	Reference
March 2018/2017EE Rev 1	Removed process for setting up single sign-on and documented removal of support for single sign-on.	--
	Added a description for the Client ID field.	page 30
	Created a new chapter on authentication.	page 35
	Significant updates to Chapter 6, "Channel Islands UI Security," including user and role information, role permissions, menus, and resources.	page 73
	General editing for clarity throughout the guide.	--
September 2017/2017EE	Merged material from System Security guide; retitled from Security and Controls User Guide to Security Admin Guide	--
	Added chapter on QAD .NET security	page 137
	Added chapter on user management security setup	page 35
	Added a description of the Session Expires Minutes field	page 26
	Added a section on Active Directory	page 55
	Added chapter on setting up secured Channel Islands resources	page 73
	Added chapter on setting up reverse proxies for Channel Islands	page 213
	Changed the directory where QAD-provided default profiles are found	page 169
	Updated some sections in the Auditing chapter	page 195
September 2016/2016EE	Added Channel Islands and System Security information.	--
March 2016/2016EE	Removed obsolete topic on Progress-level database access.	---
	Added IAQ E-Signature information to Ch. 7	page 163
March 2015/2015EE	Rebranded for QAD 2015 EE	--
March 2014/2014 EE	Rebranded for QAD 2014 EE	--
September 2013/2013.1 EE	Added new section on Disabling the Superuser Role	page 138
	Added new section on Activating Segregation of Duties from the Command Line	page 140
	Various minor changes	--
March 2013/2013 EE	Updated description for Timeout Minutes field	page 26
	Updated description for User ID field	page 52
September 2012/2012.1 EE	Rebranded for QAD 2012.1 EE	--
March 2012/2012 EE	Supplier-Withholding Tax [Entity] activity removed from Secured Items Not on Menu table.	page 62
	BCube activity removed from Secured Items Not on Menu table.	page 62

Date/Version	Description	Reference
	BReportTree activity removed from Secured Items Not on Menu table.	page 62
	BDInvoice node with activity Customer Invoice–Modify Due Date [Entity] added to Secured Items Not on Menu table.	page 62
	BERS and BERSLine activities added to Secured Items Not on Menu table.	page 63
	Generalized Code Groups added to Secured Items Not on Menu table.	page 64
	New section added on Enabling Auditing on Selected Fields.	page 203
September 2011/2011.1 EE	Rebranded for QAD 2011.1 EE	--

Introduction to Security

This section introduces the security and internal control features in your system.

Overview 2

Explains the fundamental components used to assure the preservation of confidentiality, integrity, and availability.

User and Role-Based Security Model 3

Explains the security model used by the system to integrate the different components of the system architecture, control who can access the system, and define the actions that system users can perform.

System Security 4

Describes the overall security of all the components of QAD, including servers and databases, user synchronization, and user authentication.

Internal Controls 5

Explains the mechanisms that help an organization comply with legal or regulatory requirements to reduce their exposure to potential liability imposed for violations.

Implementation Summary 6

Describes how every user must be identified in the system, given access to a domain and at least one entity in the domain, and associated with at least one role in the domain in order to gain system access.

Security and Internal Controls Programs 9

Lists the menu programs you use to define and maintain security and internal controls in your system.

Overview

The security and related internal controls operating in your system must be viewed within the context of your organization's overall security framework. While it is beyond the scope of this 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

Security properly starts with a comprehensive policy statement that:

- Demonstrates clearly management's support and commitment to security
- Defines the principal 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 are designed and implemented to support the administrative controls.

The system provides multiple types and levels of security and internal controls, which are described in this chapter. This chapter also 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. See "Security Planning Checklists" on page 7 for details.

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 the system is designed to support external requirements, including numerous controls to support 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.

User and Role-Based Security Model

The security model used by the system integrates the different components of the system architecture, controls who can access the system, and defines the actions that system users can perform.

Using security features, you can configure system login behavior, define password policies, create and maintain users and roles, as well as specify user access to domains and entities.

The guiding rule in role-based security is that access to a resource is not allowed unless it has been specifically granted. Role-based security features let you control user access to all menu-based application resources, as well as some resources that represent activities that are not directly accessed from the menu.

Using the login security features, you can secure your system from unauthorized users.

You also can configure additional types of security that provide enhanced protection for individual database records, fields, sites, GL accounts, and so on.

Note If you intend to use other components of the QAD Enterprise Application Suite that communicate with core functions through APIs, a system administrator must configure security for these add-on products appropriately. These security details are included in the relevant product documentation of the other components.

Enterprise Edition resources include:

- Standard programs, which display on the system menu as a single maintenance function. Standard programs are available in both the QAD .NET User Interface (UI) and character interface.
- Component-based functions, which display on the system menu as items with one or more associated activities. A component-based function is always associated with an activity or multiple activities. Component-based functions are available only in the QAD .NET UI.

Additionally, the Channel Islands UI is comprised of multiple types of resources, which are uniquely identifiable pieces of the product that have been designated as needing to be secured. These resources include business entities, services, browses, fields, and KPIs.

When a user logs in, the system determines the programs or functions to display on the application menu based on the user's roles in the current domain and entity. This occurs in exactly the same way regardless of whether login is from the character user interface, the QAD .NET UI, or the Channel Islands UI.

Important The various system security controls are primarily effective within an application session. The system database should be protected from any unauthorized access, not just access from within an application session. Additional controls should be considered to prevent compromise of system data using other means. See "Operating System and Progress Security" on page 20 for details.

4 QAD Security Administration Guide

During an application session, several different types of security operate at the same time.

Fig. 1.1
Types of Security

Domain/entity security restricts access based on user ID.

Role-based security prevents access to screens.

The screenshot shows the 'Sales Order Maintenance' window. It has a menu bar with 'Processes' and 'Sales Order Maintenance'. Below is a toolbar with 'Go To', 'Actions', 'Copy', 'Print', 'Preview', and 'Attach'. The main area has tabs for 'Header', 'Lines', and 'Trailer'. The 'Header' tab is active, showing fields for 'Order: SO031521', 'Sold-To: 22C1001', 'Bill To: 22C1001', and 'Ship-To: 22C1001'. Below these are 'Sold-To' and 'Ship-To' details for 'Teasdale Hospital Equipment'. The 'Details' section shows dates, pricing, and other order information. A 'Back' and 'Next' button are at the bottom right.

Field security prevents users from updating values for specific fields.

System Security

System security comprises the overall security of all the components of QAD, including servers and databases, user synchronization, and user authentication.

System Security Features

Common Implementation Features

- All network communications can be encrypted using SSL.
- Applications support user access management by allowing user accounts to be created, modified, and deactivated.
- Applications support user access management by allowing user accounts to be assigned roles (for example, roles defined in QAD Enterprise Edition).
- Users are uniquely identified by their email address, QAD username, and optionally, their Active Directory username.
- Applications support auditing by mapping user access across systems using email addresses and Active Directory usernames. All internal references use QAD usernames.
- Each QAD application is assigned a unique group within the Directory.
- Each user ID in the Directory is assigned to the appropriate QAD application group.

- Each QAD application is assigned a collection of roles (for example, roles defined in QAD Enterprise Edition) within the Directory.
- All passwords stored in the system are hashed using the PBKDF2 algorithm. Passwords are not stored when users are authenticated using LDAP.

Native Application Features

- Native applications use LDAP authentication against a Directory service using the LDAP distinguished name associated with the user.
- LDAP connections use SSL (LDAPS).
- LDAP connections are made with a specific service account (username/password).
- LDAP queries are customizable.

Progress OpenEdge Security Configuration

For information on Progress OpenEdge security, refer to the Progress documentation on security, SSL in OpenEdge, and configuring and running SSL sessions.

Internal Controls

In addition to security features, the system also has internal control features. Internal controls are mechanisms that help an organization comply with legal or regulatory requirements to reduce their exposure to potential liability imposed for violations. For example, the Sarbanes-Oxley Act of 2002 mandated that public companies must provide an assessment of the effectiveness of the organization's internal control over financial reporting.

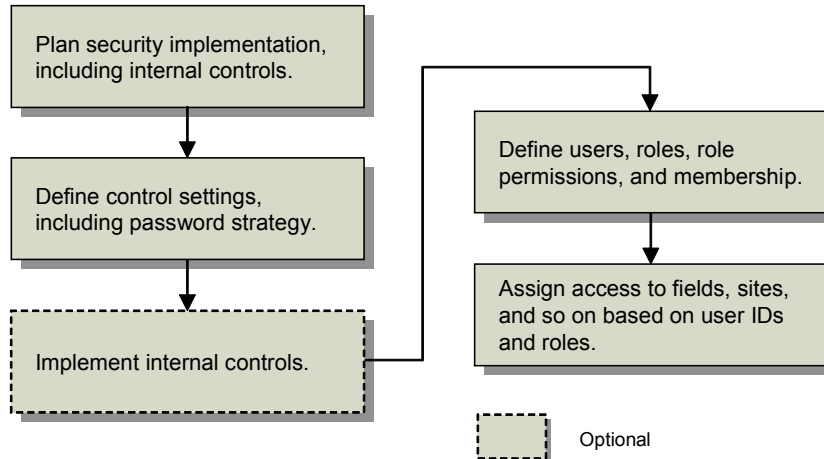
The system has these internal control features:

- Segregation of duties. Provides features that prevent a user from participating in more than two parts of a transaction or process. This is accomplished by partitioning the system application resources into mutually exclusive categories. See Chapter 8, "Segregation of Duties," on page 125.
- Electronic signatures. Provides features that require users of some system programs to enter a valid user ID and password before they can create or update records. See Chapter 9, "E-signatures," on page 163.
- Auditing. The Auditing module integrates with the Progress OpenEdge Auditing capability. You can configure your system to maintain audit trails. Audit-trail records are created and stored in audit-trail tables. They contain facts about changes made in the databases. A typical audit record includes information that helps you identify who made a change, which program made the change, when the change was made, and what the change was. You can set up these functions for all tables or you can limit the audit trail recording activity to specific tables. See Chapter 10, "Auditing," on page 195.

Implementation Summary

Figure 1.2 illustrates a workflow for implementing security and internal control features.

Fig. 1.2
Security Workflow



Establishing a Security Plan

Every user must be identified in the system, given access to a domain and at least one entity in the domain, and associated with at least one role in the domain in order to gain system access.

A number of roles are supplied with the system. These roles can be used for notification when a new customer, supplier, employee, or end user is created. These roles are provided to enable system setup; for details see the section “System-Supplied Roles” on page 64.

Use the set of checklists provided in this section as a starting point for determining the focal points to consider when establishing a security plan. See Table 1.1 on page 7.

You should consider both internal and external requirements when planning such security elements as password protection. For example:

- Does your organization have specific internal controls-related requirements that may require the implementation of segregation of duties or update restrictions?

Important By carefully planning how you will integrate your defined SOD policy with your setup of user roles, role permissions, and role membership, you may avoid SOD policy violations that require configuration rework.

- Does your organization have specific requirements regarding password aging for all its systems?
- Do external regulatory agencies set standards for 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 your QAD applications?

Other planning considerations apply if you are setting up security for a multiple-domain database.

For example, user profiles defined in User Maintenance (36.3.1) 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.

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. For more information on this topic, see [QAD Financials User Guide](#).

Implementing Your Security Plan

After planning how your security system should operate to meet your organization'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. See page 25.
- Set up users, roles, role permissions, and role membership. Depending on your overall security plan, you can define such elements as domain access and role membership, as well as enter temporary passwords for your users. See page 47.
- Set up internal controls (optional). You can reduce the complexity of implementing segregation of duties by partitioning your system resources at the same time as you define users and roles by using an iterative approach.
- Set up user access to fields, sites, GL accounts, and inventory movement codes as required. See page 107 for details.

Security Planning Checklists

Tables 1.1 through 1.3 summarize the various security controls that should be considered as part of an effective overall information security plan for the system. 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 1.1
Planning, Policies, and Procedures Checklist

Topic	Reference
Review all information about security documentation for both the system and Progress prior to installation (or software upgrade if applicable).	• This chapter • <i>Installation Guide</i> • Progress documents, including <i>Data Administration, Guide, Client Deployment Guide</i>, and <i>Programming Handbook</i>
Review all application-related files to determine the appropriate permission and ownership settings.	"Operating System and Progress Security" on page 20
Optionally, determine and document any segregation of duties policy requirement. Also document how application resources should be partitioned.	Setting Up Segregation of Duties

Topic	Reference
Document the users who should be permitted access to the system and the domains and entities to which they should have access. This step will require an in-depth knowledge of your organization's security requirements.	• "Define Users" on page 51 • "Specify Access to Domains and Entities" on page 59
Document the role or roles to which users should be assigned. This step will require an in-depth knowledge of your organization's security requirements.	"Set Up Roles" on page 61
Determine if specific users will require access to individual fields, sites, general ledger accounts, or inventory movement codes for standard application programs.	"Additional Security for Standard Programs" on page 107
Consider requirements for policies and/or procedures regarding the deactivation of old user accounts. To meet the requirements of many regulated environments, user accounts can be disabled, but not deleted, once they have been used to access the system.	"Set Up Users" on page 49
Define policies and procedures to be used to assure that user/role information will be kept current.	
Create a high-level overview of your business environment and use a top-down approach to define your segregation of duties requirements.	"Plan a Segregation of Duties System" on page 131
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 30
Decide if a simplified access approach is sufficient. This lets users log in based on operating system-level security.	"OS-Based Sign-in Security" on page 20
Define how often users are required to change passwords, and update the corresponding system security setting.	"Expiration Days" on page 31
Define procedures for failed login attempts, 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	• "Security Control" on page 25 • "Monitor System Security" on page 33
Define password policies and procedures, including password composition, length, expiration, and reuse of previous passwords.	"Create a Password Strategy" on page 30
Define appropriate policies and procedures for users requiring that application sessions be locked using a screen saver or comparable mechanism whenever the user leaves the session unattended.	"Client-Level Security" on page 22

Table 1.2
Progress and Operating System Checklist

Topic	Reference
Determine requirements for Progress-level schema security to control access to application database tables.	"Progress-Level Database Schema Controls" on page 22
Consider disallowing Progress-level table and field access for the blank user ID	"Progress Editor Access" on page 21

Topic	Reference
Determine the period of inactivity after which a system session should be terminated. For each device used to access the system, ensure 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 application session.	"Client-Level Security" on page 22
Determine whether multiple users share a common workstation to access the system and whether appropriate operating system functionality exists to adequately support security.	Operating system documentation

Table 1.3
System Security Parameters, Setup, and Processes Checklist

Topic	Reference
Verify and update relevant system control program settings, especially those for security.	"Security Control" on page 25
Define users assigned to the security administrator role, who will receive e-mail notification of security events such as failed logins exceeding a defined threshold.	• "Administrator Role" on page 28 • "Maximum Access Failures" on page 28
Update system 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 login attempts	"Create a Password Strategy" on page 30
Determine how system security should be implemented to protect the integrity of database records. For each site, GL account, and so on, specify the appropriate users authorized to access data.	"Additional Security for Standard Programs" on page 107
Review users and roles for potential segregation of duty issues and adjust assignments as appropriate.	Setting Up Segregation of Duties

Security and Internal Controls Programs

Table 1.4 lists the menu programs you use to define and maintain security and internal controls from the QAD .NET UI (or Character UI). The system uses a combination of Progress-based (.p) and component-based functions that have the form Component.Activity, such as BRole.Create, which is the create activity of the role component.

Table 1.4
System Security Menu (36.3)

Program No.	Description	Program Name
36.3	System Security Menu	
36.3.1	User Maintenance	mgurmt.p
36.3.2	User Inquiry	mguriq.p
36.3.3	User Password Maintenance	mgurmtp.p
36.3.4	User Domain/Entity Access Maintain	BUser.Modify

Program No.	Description	Program Name
36.3.5	User Domain/Entity Access View	BUser.UsrCompanyDomainAccess
36.3.6	Role Maintenance	
36.3.6.1	Role Create	BRole.Create
36.3.6.2	Role Modify	BRole.Modify
36.3.6.3	Role View	BRole.View
36.3.6.4	Role Delete	BRole.Delete
36.3.6.5	Role Permission Maintain	BRole.Permissions
36.3.6.6	Role Membership Maintain	BUserRole.Maintain
36.3.6.8	Role Permissions View	BRole.RoleDefinition
36.3.6.9	Role Membership View	BUserRole.RoleMembership
36.3.6.10	User Access View	BUser.Useraccess
36.3.6.11	Role Export	BRole.Export
36.3.6.12	Role Import	BRole.Import
36.3.7	Update Restrictions Menu	
36.3.7.1	Inv Transfer Restriction Maint	mguritmt.p
36.3.7.2	Inv Detail Restriction Maint	mguridmt.p
36.3.7.3	Unplanned Iss/Rct Restrict Maint	mgurirmt.p
36.3.7.5	PO Restriction Maintenance	mgurpomt.p
36.3.7.6	PO Receipts Restriction Maint	mgurprmt.p
36.3.7.8	SO Restriction Maintenance	mgursomt.p
36.3.7.9	SO Shipments Restriction Maint	mgurssmt.p
36.3.7.13	DO Restriction Maintenance	mgurdomt.p
36.3.7.14	DO Shipments Restriction Maint	mgurdsmt.p
36.3.7.15	DO Receipts Restriction Maint	mgurdrmt.p
36.3.7.17	SSM Restriction Maintenance	mgursmmt.p
36.3.7.19	Update Restriction Report	mgurrrp.p
36.3.13	Operational Security Menu	
36.3.13.1	GL Account Security Maintenance	mgacsmt.p
36.3.13.2	GL Account Security Report	mgacsrp.p
36.3.13.8	Site Security Maintenance	clsismt.p
36.3.13.9	Site Security Report	clsisrp.p
36.3.13.13	Inventory Movement Code Security	sosimt.p
36.3.13.14	Inv Mvmt Code Security Browse	gpbr502.p
36.3.15	Field Security Menu	
36.3.15.1	Field Security Maintenance	mgflpwmt.p
36.3.15.2	Field Security by Role	mgflgpmt.p
36.3.15.3	Activated Field Security Report	mgflpwrp.p
36.3.15.4	Dictionary Field Security Report	mgfldcrp.p
36.3.15.6	Component Field Security Create	BFieldSecurity.Create
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

Program No.	Description	Program Name
36.3.22	User Access by Application Inquiry	lvusriq.p
36.3.23.12	User Password Force Change Util	utfrcpsw.p
36.3.24	Security Control	mgurpmmt.p

Security Overview

This section discusses the security features available in your system:

***Role-Based Access Security* 14**

Explains roles, role permissions, role membership, and additional types of security.

***Password Management* 16**

Describes how passwords can be managed using Security Control settings.

***Sign-in Security* 17**

Outlines types of sign-in, domain and workplace security, and different types of security control.

***Operating System and Progress Security* 20**

Describes different types of operating system and progress security, including details on Progress Editor and Progress-level database information.

***Client-Level Security* 22**

Describes potential client-level security settings that are available with some operating systems.

***QAD .NET UI Security* 23**

Explains how QAD .NET UI supports certain additional customization and security options.

Role-Based Access Security

Role-based access security is a method of assigning system access to authorized users based on their role in the organization. Roles are created to perform various job functions, and the permissions required to carry out those job functions are granted to the different roles. Individual users are then assigned one or more roles in the system, giving them access to the areas of the system for which their roles are authorized.

Role-based access security operates through the use of several key components:

- Roles
- Role permissions
- Role membership

The system has additional types of security that can be configured for standard programs, component-based functions, and the Channel Islands User Interface.

Roles

A role is a logical subset of activities that describes a user's business function or set of responsibilities within a business enterprise. You can define as many roles as required in the system in order to model your business processes. Roles are created by using Role Create (36.3.6.1).

Users in the system have at least one role—and possibly several roles. In addition, the same role can be associated with several users. Before users can sign in to the system, they must be associated with at least one role.

A role, when associated with a set of application resources, defines the tasks or activities a user can perform when using the system. The process of associating application resources to a role defines role permissions. For details see “Role Permissions”.

Roles operate within the context of the domains and entities to which the user has been granted access. This concept is known as role membership. For details see “Role Membership” on page 15. A user with multiple roles has access to the sum of the resources assigned to each.

Role Permissions

Role permissions are defined by assigning a set of application resources to a role using Role Permissions Maintain (36.3.6.5) in the QAD .NET UI or Role Permissions in the Channel Islands UI.

- For component-based functions, role permissions control the ability to use the various types of activity—approve, create, delete, read, and write.
- For standard programs, role permissions control the ability to execute those programs.

Note Access control can also be defined for fields, sites, GL account updates, and inventory movement codes using user ID, role, or a combination. For details see “QAD .NET UI Security” on page 99 and “Channel Islands UI Security” on page 73.

The QAD .NET UI application resources defined in the system display in a tree layout similar to the way the menu looks in the .NET User Interface. To define role permissions, you select the resources to assign to the role. Once role permissions and role membership have been defined, when a user opens a workspace, only the application resources associated with that role display on the application menu. When a user has more than one relevant role, the application resources that display are essentially the sum of the user roles.

Example Sophie Woods has been assigned the roles Project Manager and Accountant. The Project Manager role allows her access to the Customer View function. The Accountant role allows her access to the Customer Invoice Create function. Consequently, the following menu choices display when she signs in:

Customer View

Customer Invoice Create

The role-based security that is defined for a function also applies to any associated functions that are available on the Go To menu for which a user has been granted access. For example, if you are modifying data in the Customer Invoice Create function, the Go To menu for that function displays related functions—Daybook Create, for example—for which you have appropriate permissions.

Role-based security also applies to parts of the system that do not have a user interface—for example, Web services and API calls, as well as daemons. For more information on daemons, see [QAD System Administration User Guide](#).

Role Membership

Role membership associates users and roles, as well as the domains and entities in which that role operates. Use Role Membership Maintain (36.3.6.6) in the QAD .NET UI and User Access in the Channel Islands UI to create and maintain role memberships.

For each domain, access can be restricted to one or more entities in the domain. In essence, role membership defines the *context* of a particular role by specifying the meaning of a role within a specific domain and entity.

A user's role always operates within the context of a domain and entity; you cannot set access at the domain level. You must explicitly grant access to users to each entity within the domain. However, entity-level access has meaning in most cases only within financial functions. Users who will be working exclusively with operational functions such as sales, shipping, and manufacturing are typically given access to the primary entity of the domain.

Example Sophie Woods has the role Project Manager for all entities in the Australia domain. When she accesses the Australia domain, the access privileges for her Project Manager role apply for all entities within the domain. Her privileges do not apply if she signs in to a different domain.

Example Roger Spencer has been assigned the role Accountant, but only for the entity 001 Fit & Co Pacific in the Australia domain; his role privileges do not apply for other entities in the Australia domain or any other domain.

Certain standard programs, described in the next section employ a user ID, role, or sometimes both in order to control access, as in previous versions of QAD applications.

Additional Types of Security

Some additional types of security can be configured for standard programs and component-based activities.

Additional Security for Standard Programs

The system has several types of security that apply to operational programs only. In these programs, security is defined by user ID, role, or a combination of both.

- Field Security Maintenance (36.3.15.1) limits who can update specific fields. For field security, specify a user ID.
- Update restrictions functions on the Update Restrictions menu (36.3.7) limit who can update specific records and create specific issue, receipt, and transfer transactions.
- GL Account Security Maintenance (36.3.13.1) restricts access to GL accounts from operational functions. Specify any combination of user IDs or roles.
- Site Security Maintenance (36.3.13.8) limits who can create inventory transactions at secured sites. Specify any combination of user IDs or roles.
- Inventory Movement Code Security (36.3.13.13) lets you grant or deny user access to shippers and other transactions using specific movement codes at a site. Specify any combination of user IDs or roles.

For details about setting up operational programs, see “Additional Security for Standard Programs” on page 107.

Additional Security for Channel Islands

The system has additional security for the Channel Islands UI. This security, which is defined by role, is managed through the Channel Islands UI.

- Granular-level security allows you to grant various levels of access to different roles for all defined resources, including business entities, individual reports, browses, and KPIs.
- Field security limits which roles have read and write access to fields and field groups.
- Channel Islands is designed to operate over the internet with a secure UI and secure APIs.
- All actions on the Channel Islands UI are determined by role security.

For details on setting Channel Islands security, see “Channel Islands UI Security” on page 73.

Password Management

The system 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 needed to meet requirements.

You can specify:

- 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

For details, see “Create a Password Strategy” on page 30.

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 sign 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 sign in using the temporary password—subject to the parameters defined in Security Control.

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 sign in. Force Password Change Utility (36.3.23.12) makes all users or specified roles change their passwords. For details, see “Update Passwords” on page 57.

Sign-in Security

The following types of security are enforced at sign in:

- Sign-in security determines whether a user can sign in to an application session based on their user ID and password. This level of security is always active, although how it is implemented depends on settings in Security Control.

For example, system administrators can choose to allow valid users to sign in to the QAD application based on operating system-level access. See “OS-Based Sign-in Security” on page 20 for details.

Note You also should consider additional access security options at the operating-system and Progress levels. See “Operating System and Progress Security” on page 20 for details.

- Domain/entity security limits individual user access to the domains and entities identified in User Domain/Entity Access Maintain (36.3.4). If using the .NET UI, users can open other workspaces in order to access domains and entities for which they are authorized.

These two types of security are closely related and work together to ensure that users can only access the business areas that they have been authorized.

Workspace Security

Access to domains and entities is controlled at two points:

- During system sign in
- During the application session

When users start the system, they submit user credentials using the sign in dialog box.

The client authenticates the user by calling the authentication service. If a user's identity cannot be verified, sign in to the system fails. This authentication takes place during sign in for the character UI, the QAD .NET UI, and the Channel Islands UI. The system next checks to see if the user has access to any domains and entities defined in User Domain/Entity Access.

This step varies based on the user interface:

- In character, the system checks to see if the user has an assigned domain. If not, an error is generated, and sign in is refused. If only one assigned domain is found, sign in to that domain is automatic. A user with access to more than one domain can choose from a list. The one marked as default in User Domain/Entity Access displays at the top of the list.
- In .NET UI and Channel Islands UI, the authentication service creates a session for the user, and returns a session ID to the .NET UI. The .NET UI uses the session ID to initialize any workspaces (domain/entity combination). By default, this is the workspace that was active when the user signed out of a previous session. If no previous session exists, the default domain is used.

Note Sign in to the .NET UI can be successful even when the user is not assigned to a workspace. This is because the .NET UI is a container for multiple applications and also provides access to system administration functions that are not part of any specific application.

Changing domains also differs depending on the UI:

- In the .NET UI and the Channel Islands UI, a user with access to more than one domain or more than one entity in a domain switches from one to another by opening a different workspace.
- In the character UI, users switch domains by using Change Current Domain (36.1.1.1.10). This automatically switches to the primary entity of the new domain.

At no time can a user access an entity that is not authorized in their user record. In the .NET UI, these workspaces do not display for selection; in the character UI, attempting to switch to an unauthorized domain or entity displays an error message. See “Specify Access to Domains and Entities” on page 59.

When a user exits the .NET UI, the active workspace is saved and displays when that user signs in again. In the character UI, the default domain assigned to the user in User Domain/Entity Access always displays by default.

For details about using and managing workspaces, see [Introduction to QAD Enterprise Applications User Guide](#).

Sign In and Security Control

Use Security Control (36.3.24) to define additional security measures related to system sign in.

Note Single sign-on is not supported in this release of Enterprise Edition. The Single Sign On Enabled check box remains active in Security Control, but you should not select it. If you do select the check box, you will receive Active Directory errors and be prompted for sign-in credentials.

If a user enters an invalid combination of user ID and password, 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 disabled, and system administrators are notified by e-mail. The sending address of the e-mail includes the

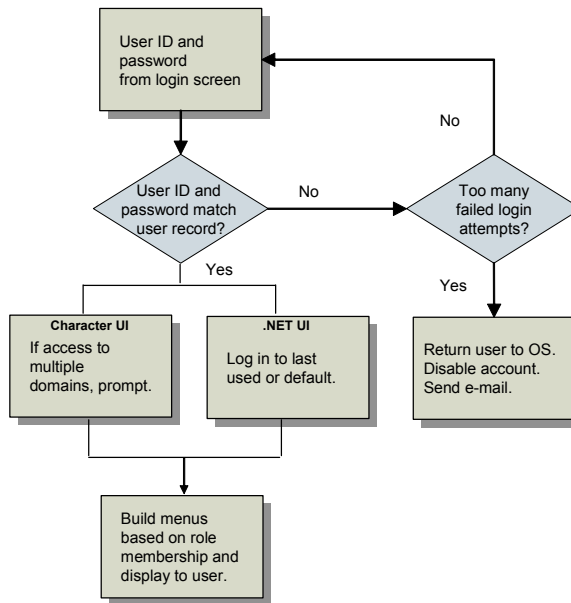
operating system ID of the user who attempted to access your QAD application. Figure 2.1 illustrates how this process occurs during sign in. Use the User Account Status Report (36.3.23.2) to view the status of system users.

To completely or partially bypass system sign-in security, you can configure the system to allow users to access the system based on operating system user ID. See “OS-Based Sign-in Security” on page 20.

Depending on the setting specified in Security Control, the system maintains historical records of successful and failed sign-in attempts. Use Logon Attempt Report (36.3.23.1) to view sign-in history.

Note In order for the time zone to be properly recorded during sign in and password change, the server time zone must be specified in Database Control (36.24.1).

Fig. 2.1
Sign-in Validation from Sign-in Screen



Using sign-in security, you can:

- Effectively separate QAD application security from the operating system security (unless you choose to control access from the operating system level). The user ID in your QAD application does not have to be the same as the user ID referenced by UNIX or Windows. See “OS-Based Sign-in Security” on page 20.
- 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 QAD applications presents an additional barrier to an unauthorized user.
- Track unsuccessful sign-in attempts to identify possible unauthorized efforts to access the system.

OS-Based Sign-in Security

System administrators can control user access to the character interface directly from the operating-system level using the Enforce OS User ID field in Security Control (36.3.24).

If you are not using an application password, using the Enforce OS User ID feature lets you essentially bypass application sign-in security completely and rely on operating-system security for your character-based users.

The .NET UI and Channel Islands UI support Microsoft's Active Directory authentication for use with the Enforce OS User ID field. With Active Directory support, user passwords can be centrally managed. User accounts must be created in the QAD system, and the User ID must match the Active Directory User ID. Note that in the QAD system, the User ID is limited to eight characters.

Important Regardless of this setting, users signing in through .NET UI and the Channel Islands UI must enter a valid user ID and password to access the system.

When the Enforce OS User ID check box is selected, the default user ID displayed in the sign-in screen is the same ID used by the operating system, and the user cannot change it. This must still be a valid system user ID defined in User Maintenance (36.3.1).

Enforce OS User ID uses Windows environment variables to verify user credentials. An unauthorized user may potentially be able to reset the %USERNAME% environment variable in order to gain access to the system, masquerading as a different user. You should consider this issue carefully when defining your security model.

Subsequent processing depends on whether a password is required for the user:

- If no password is specified in the system user record, sign 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 user passwords for the application to blank, be careful if the Enforce OS User ID check box is ever cleared. If you do so without reentering passwords in user records, anyone can gain access to the system by entering just a user ID. When you clear this check box, the system displays a message to warn you of a potential security compromise. In addition, if using the .NET UI, it is not recommended that you reset user passwords for the application to blank. It is relatively easy to create a new user on an existing Windows machine with an ID that matches one in the application.

Operating System and Progress Security

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 system controls, you should consider additional security at the operating system and Progress levels.

At the operating system level, all application-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
- Configuration files (*.config)
- Files used to execute system implementation functions such as the QAD deployment tool
- Files that are part of the QAD .NET User Interface

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 the application
- Capabilities to directly read, modify, and delete database records
- Compiling custom code on unprotected databases
- Accessing an application database directly from Progress

Progress Editor Access

One area of potential security exposure is related to the Progress Editor. Access to the Progress Editor from your QAD application is often essential in troubleshooting technical problems. At the same time, once a user has accessed the Progress Editor, system data can be significantly exposed.

Access to the Progress Editor is available from menu 36.25.80, `mgeditor.p`. You can use roles to limit access to the Progress Editor in the same way as any other application menu programs. Using Role Permissions Maintain, assign appropriate access permissions to the roles you want to be able to access the Progress Editor, and then assign these roles to legitimate Progress Editor users.

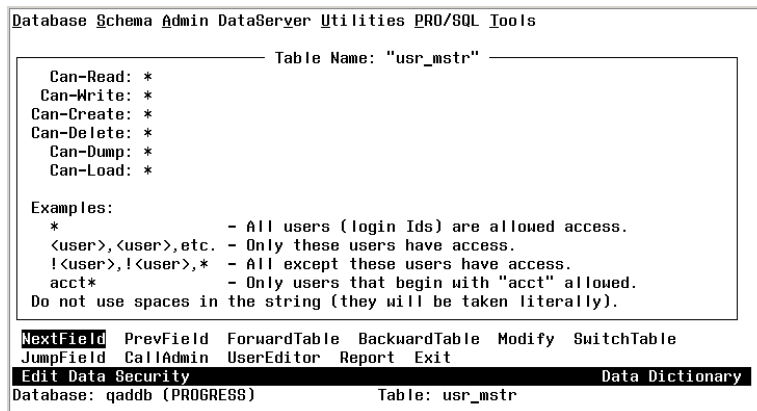
Another related control that should be considered is to disallow privileges for users connecting to the application database with a blank user ID. The Disallow Blank User ID Access option on the Progress Database|Admin|Security menu is available for this purpose. See the “Maintaining Application Security” section in the *Progress Client Deployment Guide* for details.

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 details.

Progress-Level Database Schema Controls

Progress-level security controls should also be considered for protecting the application 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. 2.2
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.

To provide protection against this exposure, consider using the Progress PROUTIL function DBAUTHKEY to set a key for a Progress database. See the *Progress Database Administration Guide* for details.

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.

Client-Level Security

Depending on the operating system of the machines that are running application sessions, you may be able to combine an application security setting with operating system features to create an additional security layer at the client 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 signs a user out of an application session. Primarily used to reduce the system load resulting from users who stay signed 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 signed in when they go to lunch and leaving an open session that might be accessed by unauthorized individuals. See the section “Idle Timeout Minutes” on page 26.

In the character UI, this feature applies only when the application is displaying a menu, rather than when a program is executing. In the .NET UI, time out is applied regardless of whether the user is displaying a program screen.

Note To add client security for times when a user leaves a computer unattended while a program is running, you can use operating system features.

Windows Systems

In many environments, users run the application on a Windows system; for example, character sessions using a terminal emulator, or the .NET UI. 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 the application sign in—to turn off the screen saver.

For details, refer to your Windows system documentation.

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. Refer to your operating system documentation for details.

Non-Windows Systems

Many standard UNIX machines—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 machine for details.

QAD .NET UI Security

The QAD .NET UI supports external customized menus defined in XML. The ability to customize menus allows you to add content—the QXtend plug-in, for example—outside of standard programs and functions.

The items on external menus are not filtered unless a security constraint is added to the menu; this is achieved by manually editing the menu extension configuration file. Security constraints can be placed on the XML file by user or role.

For details, refer to the installation guide.

Security Control

This section discusses how to set up basic security in your system.

***Define General Security Settings* 26**

Describes the frames of Security Control and what they are used for.

***Create a Password Strategy* 30**

Describes how to use the Password frame to specify password settings, such as complexity requirements and expiration dates.

***Set Up E-mail Notifications* 32**

Describes the circumstances under which the system can automatically send e-mail notifications to users.

***Monitor System Security* 33**

Describes the automatic features used to help administrators control and monitor security activities.

Define General Security Settings

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:

- Each time a field is updated, the system notifies administrators by e-mail. See “Set Up E-mail Notifications” on page 32 for details.
- 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 the Progress Editor, to modify that record.

Fig. 3.1

Security Control (36.3.24), Initial Frame

Idle Timeout Minutes. Specify a number of minutes after which the system automatically signs out inactive sessions. Set a value in this field to minimize unnecessary overhead on busy systems.

Note If a nonzero value is entered in this field, the Timeout daemon must also be configured and started. For more information on daemons, see [QAD System Administration User Guide](#).

The field also can be used as part of an overall security strategy to prevent users from inadvertently allowing access to unauthorized individuals. See “Client-Level Security” on page 22 for details.

If you enter a value, when the system considers a session inactive depends on the UI:

- In the character UI, the time out is applied only when a menu is displaying, such as Item Data Menu (1.4) If the user is executing a program—Item Master Maintenance (1.4.1), for example—a session is never automatically signed out.
- In the .NET UI, the time out is applied regardless of what the signed-in user is doing. This is because the load on system resources for inactive users is much greater in the .NET UI.
- This setting does not affect the Channel Islands UI.

For a particular user, you can use Generalized Codes Maintenance to set a timeout that is different than the general timeout in Security Control. To do this, use the sess_timeout_min field in Generalized Codes Maintenance, specify the user ID in the

Value field, and specify the timeout in minutes in the Comments field. If you specify 0 (zero) as the timeout, the user's session will never expire. This feature is particularly useful for a user who runs batch processes.

You can only use Generalized Codes Maintenance to set a timeout for one user ID. If you try to enter a timeout record for more than one user ID, an error is displayed. For more information on generalized codes, see [QAD System Administration User Guide](#).

Session Expires Minutes. This field indicates how long the session can be used before it expires. It is not related to the Idle Timeout Minutes setting. Set this field to a large value, such as 1,440 minutes (24 hours). When the field is set to 0 (zero), sessions never expire.

Enforce Licensed User Count. Use this option to implement enforcement of the total number of users, sessions, or transactions allowed based on your license agreement.

Not selected (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.

Selected: 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 sign in to the system
- When users attempt to use separately licensed applications or non-registered 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 character sessions for the application based on their operating system sign in. See “OS-Based Sign-in Security” on page 20 for details.

Not selected: Users must always enter a valid user ID and password.

Selected: Depending on password parameters defined in Security Control, valid users defined in the system may be able to access the application directly without entering sign-in information.

Note The Enforce OS User ID option cannot be selected if the Single Sign-On Enabled option is selected.

Header Display Mode. Use this field to control the information that displays in the menu and program title bars of programs in the character interface. Valid values are:

0 (Display Date). The menu title bar displays the name associated with the current domain followed by the current database name defined in Database Connection Maintenance (36.6.1). 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 3.2).

Fig. 3.2
Header Display Mode 0



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 sign-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 sign-in ID of the current user (see Figure 3.3).

Fig. 3.3
Header Display Mode 1



2 (Display Date and 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 3.4).

Fig. 3.4
Header Display Mode 2



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 sign-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 sign-in ID of the current user (see Figure 3.5).

Fig. 3.5
Header Display Mode 3



Some regulatory environments may require the name associated with the user ID of the signed-in user to be available from any program. In the character interface, you can use the Ctrl+F key combination to review this information and other context details.

Maximum Access Failures. Enter the maximum consecutive failed sign-in attempts allowed before the system disables the user's sign-in ID. When an account is disabled, the system sends an e-mail message to the system administrator. See "Set Up E-mail Notifications" on page 32 for details.

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 disables the user ID.

Administrator Role. Specify the role assigned to system administrators. The members of this role receive e-mail notifications when specific security and controlled events occur; for example:

- When a user account is disabled for too many failed sign-in attempts. See page 32 for details.
- If you are using electronic signatures, when an electronic signature profile is activated or a user account is disabled for too many failed signature attempts.
- When an update is made in Security Control. See page 32 for details.

Typically, the administrator role includes a 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 system administrators when security- and internal control-related events occur.

Note The system first attempts to use the e-mail definition specified for the signed-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. For more information on setting up e-mail, see [QAD System Administration User Guide](#).

Single Sign-On Enabled. Single sign-on is not supported in this release of Enterprise Edition. The check box remains active but you should not select it. If you do select the check box, you will receive Active Directory errors and be prompted for sign-in credentials.

Logon History Level. Indicate the level of system-maintained sign-in history.

None (the default): Sign-in history is not maintained.

Failed: Sign-in history is maintained only for failed sign-in attempts.

All: History is maintained for all sign-in activity.

Particularly in highly regulated security environments, you can use sign-in history information as part of an overall access monitoring effort. Use Logon Attempt Report (36.3.23.1) to view sign-in history. See “Monitor System Security” on page 33.

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.

Enabled 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-Disablement Reason field.
- Reason codes entered manually in the Enabled Reason field in User Maintenance. See “Enabled Reason” on page 56 for details.

Example You could use Reason Codes Maintenance to create the following reason codes associated with type USER_ACT:

- AUTO. The system automatically disabled the account. You could enter this in Auto-Disablement Reason.
- REACT. The system administrator has manually re-enabled the account.
- NEW. The system administrator has added the account for a new user.
- LEFT. The user is no longer with the organization, and the system administrator has disabled 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 Enabled Reason field in the user record of the default system user, mfg. 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-Disablement Reason. Enter the reason code the system enters in user records when it automatically disables a user account. This occurs when the user reaches the number of consecutive failed sign-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.

Client ID. The client ID is required to create tokens for session management. This value is automatically populated during installation and is linked to Client ID Maintenance (36.3.12).

Enforce. Check box not in use.

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.

Note If you are using LDAP, this section does not apply because password management is done externally.

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 the application based directly on operating system security, do not define any password parameters; select the Enforce OS User ID check box in the initial frame of Security Control. To default the user ID from the operating system but still require a password for the application at sign in, select the check box and specify password parameters as needed. See “OS-Based Sign-in Security” on page 20.

Fig. 3.6
Security Control, Password Frame

The screenshot shows the 'Password' configuration frame in the Security Control application. It contains several input fields for defining password requirements:

- Minimum Length: 0
- Min Numeric Characters: 0
- Min Non-Numeric Characters: 0
- Minimum Reuse Days: 0
- Minimum Reuse Changes: 0
- Password Creation Method: No
- Password Expiration Days: 0
- Warning Days: 0

At the bottom right of the frame are two buttons: 'Back' and 'Next'.

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.

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 Force Password Change Utility (36.3.23.12) to force users to change their passwords at the next sign in. New passwords must meet the updated structure requirements. See “Monitor System Security” on page 33.

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. For details on password maintenance, see “Update Passwords” on page 57.

- 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 “Set Up E-mail Notifications” on page 32.

Note All passwords created using the specified method are temporary, single-use passwords. The user is forced to change this password at the first sign 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 application 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. The date is printed in Universal Time, Coordinated (UTC). For more information on the time stamping of transactions outside domains, see [QAD System Administration User Guide](#).

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 sign in and can optionally update their passwords immediately or, depending on menu access, update them in User Password Maintenance.

Set Up 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 sign-in attempts exceeds the number specified in Security Control, the system generates and sends e-mails to members of an administrator role. The e-mail text is similar to the following:

The purpose of this email is to inform you that a user has been disabled 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 role identified in Security Control.

User ID disabled for exceeding max logon failures allowed: *User ID*

This e-mail was automatically generated from an application process. If you have any questions about this e-mail, contact the 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 the Update Password check box is selected 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 application password. You have been sent this e-mail because Security Control has been set up to e-mail autogenerated temporary passwords.

Your temporary application password is: *password*.

You will be forced to change this password at next logon.

This e-mail was automatically generated from a QAD process. If you have any questions about this e-mail, contact the system administrator. Do not reply to this e-mail.

- When any field or check box is updated in Security Control, the system generates and sends e-mails to members of the administrator role. The e-mail text is similar to the following:

The Security Control menu program has been used to change the security configuration of QAD. Please review this information carefully to ensure that these changes will not compromise the system security. You have received this email because you are an Administrator identified in Security Control for QAD.

Changes made by user: jnw

Changed Field: old, new

=====

Administrator Role: 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 a QAD process. If you have any questions about this email, contact the QAD 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 Role 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.

Monitor System Security

Particularly in environments where security procedures are subject to regulatory controls, system administrators need methods of tracking security-related events.

The system 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 reenabled it.
- When an account is disabled, the e-mail system can automatically notify system users that have been assigned an administrator role. 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. Force Password Change Utility (36.3.23.12) lets the administrator force users to update their passwords based on role, domain, and/or the date of the last change.
- Depending on the level of sign-in history specified in Security Control, use Logon Attempt Report (36.3.23.1) to track when sign-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 sign in, as well as the date, time, server time zone, and other data relevant to the sign-in event. (If you are using electronic signatures, E-Signature Failure Report (36.12.7) lets you monitor unsuccessful signature events.)

Example You can set up batch processing to run this program each morning to identify all failed sign-in attempts on the previous day.

- Each time a user account is enabled or disabled, the Enabled Reason field in User Maintenance must be updated. This happens automatically when an account is disabled as a result of excess unsuccessful sign-in attempts. Otherwise, the administrator must enter a reason code manually.

Authentication

This section describes how to set up authentication for your system.

Overview 36

Describes authentication.

User Authentication 36

Describes how the system validates the identity of a user.

API Authentication 46

Describes the methods that can be used for API authentication.

Overview

Authentication is a process that ensures and confirms a user's identity. When logging in to the system, users provide their usernames and passwords for authentication. The combination of username and password is used to authenticate access. Authentication is not the same thing as authorization, which determines what a user is able to see and what tasks that user can complete.

User Authentication

User authentication validates the identity of a user. QAD supports user validation through the following methods:

- Lightweight Directory Access Protocol (LDAP)
- Internal

LDAP Authentication

LDAP is a well-known standard for connecting to directory services to access common enterprise services such as authentication, user, and group information. LDAP authentication should not be confused with single sign-on (SSO), because users still must enter their username and password. Centralizing authentication reduces the administrative burden of enforcing password policies and simplifies the login experience for end users by allowing the same credentials to be used across applications and enterprise services. This type of external password management is considered a best practice.

LDAP authentication can be configured to communicate with a directory service such as Active Directory or OpenLDAP, and supports multiple LDAP providers. A user can be associated with only a single LDAP provider at a time.

Internal

Enterprise Edition offers an internal authentication mechanism. QAD stores user passwords in a database and uses the PBKDF2 algorithm for password hashing to better protect against hackers reverse engineering the passwords.

Directory Services Markup Language Service

Directory Services Markup Language (DSML) provides web-services support on top of the LDAP protocol. It represents directory service information in XML syntax.

QAD provides a required DSML Service as an interface between the various QAD applications and the Directory. The information provided to a QAD application from the DSML Service includes a list of all users who can access the application, along with the role memberships of each user. Each QAD application requires a patch that enables it to communicate to the DSML Service and to synchronize user information based on the user information in the Directory.

During user synchronization, a QAD application makes a DSML search request and then receives a DSML search response. Any data needed for user provisioning not included in the DSML response can be supplied by an attribute mapping file.

To configure user synchronization in an environment managed with the YAB console:

- 1 Configure Java Keystore.
- 2 Install DSML Gateway.
- 3 Review and Update Directory to QAD Database Mappings.
- 4 Download QAD .NET UI.
- 5 Configure SYNC reason code.
- 6 Configure Alternate Country Code.
- 7 Verify LDAP Instance Definition for DSML Gateway Using User Sync.
- 8 Test LDAP.

Configure Java Keystore

A secure connection between the DSML gateway and the Active Directory requires a secure location for signed certificate storage. QAD recommends using a Java keystore (`keystore.jks`) file in a convenient location for the environment. Note the full path to the `keystore.jks` file. You will need it when you configure the DSML gateway.

Note For detailed information on setting up a Java keystore, see Java documentation.

Follow these high-level steps to configure the Java keystore:

- 1 Create a keystore file to store the server's private key and SSL certificate.
- 2 Generate a Certificate Signing Request (CSR) required by the certificate provider.
- 3 Get an SSL certificate and a Primary Intermediate CA certificate file from a CA vendor (examples include GeoTrust and Verisign/Symantec).
- 4 Import the Primary Intermediate certificate (`primary.p7b`) into the Java keystore.
- 5 Import the SSL certificate into the Java keystore.
- 6 Validate the keystore entries.
- 7 To find the configurable properties for QAD, enter:
`yab help keystore`

Install DSML Gateway

The YAB console supports installing and configuring the DSML Gateway (Configure OpenDJ DSML Gateway).

- 1 Open the `build/config/configuration.properties` file.
- 2 Configure the basic LDAP settings:
`webapp.opendj.ldap.host=`. The host name of the underlying directory server.

webapp.ldap.port=. The LDAP port of the underlying directory server. Default: 636. You can change this port to 389 for plain text during debugging, but use port 636 to secure the connection.

webapp.ldap.usessl=. Indicates whether *ldap.port* points to a port listening for LDAPS (LDAP/SSL) traffic. true or false

webapp.ldap.truststore.path=. The trust store used to verify certificates when using secure connections. If you want to connect using LDAPS or StartTLS, and do not want the gateway blindly to trust all certificates, then you must set up a trust store. Not used by default.

webapp.ldap.truststore.password=. The trust store password. If you set up and configure a trust store, then you need to set this. Not used by default.

webapp.ldap.isactivedirectory=. Designate whether Active Directory is used. true or false

webapp.ldap.domains=. An optional, comma-delimited list of valid domains.

webapp.ldap.description=. A description of the OpenDJ Instance.

- 3 Update your environment. To run only the specific steps related to the DSML Gateway, enter:

```
> yab webapp-ldap-update
```

```
> yab ldapinstance-ldap-create
```

To update your entire environment, enter:

```
> yab update
```

Setting Up Multiple LDAP Services

The previous settings support a single LDAP service. When multiple services are required, use the following steps as an example.

- 1 Open the `build/config/configuration.properties` file.

- 2 Add the new `ldap` instance for a second LDAP service.

```
@extends webapp._base
```

- 3 Configure the web app settings.

```
webapp.ldap2=
```

Note Do not enter a value for `webapp.ldap2`. This is the YAB configuration syntax for defining a new instance of the `webapp` type. This example creates “`ldap2`” `webapp`. This token can be any valid identifier, but ensure that the “`type`” is defined as “`ldap`.”

webapp.ldap2.context=. The name of the `webapp` that gets deployed; in this example, `ldap2`.

webapp.ldap2.application=. A parameter required for YAB. Leave as `${packages.ldap-dsml.dir}`

webapp.ldap2.tomcat=. A parameter required for YAB. Leave as `tomcat.default`

webapp.ldap2.upgrade.includes=. A parameter required for YAB. Leave as `WEB-INF/web.xml`

webapp.opendj2.type=. *opendj*

webapp.opendj2.ldap.host=. The host name of the underlying directory server.

webapp.opendj2.ldap.port=. The LDAP port of the underlying directory server. Default: 636.

webapp.opendj2.ldap.userdn=. The DN used by the DSML gateway to bind to the underlying directory server.

webapp.opendj2.ldap.userpassword=. The password used by the DSML gateway to bind to the underlying directory server.

webapp.opendj2.ldap.authzidtypeisid=. Required boolean parameter specifying whether the HTTP Authorization header field's Basic credentials in the request hold a plain ID, rather than a DN. This parameter can help you set up the DSML gateway to do HTTP Basic Access Authentication, given the appropriate mapping between the user ID and the user's entry in the directory. If set to true, then the gateway performs an LDAP SASL bind using SASL plain, enabled by default in OpenDJ to look for an exact match between a uid value and the plain ID value from the header. In other words, if the plain ID is bjensen, and that corresponds in the directory server to Babs Jensen's entry with DN uid=bjensen,ou=people,dc=example,dc=com, then the bind happens as Babs Jensen. Note also that you can configure OpenDJ identity mappers for scenarios that use a different attribute than uid, such as the mail attribute.

Default: false

webapp.opendj2.ldap.usessl=. Indicates whether ldap.port points to a port listening for LDAPS (LDAP/SSL) traffic. true or false

webapp.opendj2.ldap.usestarttls=. Leave blank.

webapp.opendj2.ldap.truststore.path=. The trust store used to verify certificates when using secure connections. If you want to connect using LDAPS or StartTLS, and do not want the gateway blindly to trust all certificates, then you must set up a trust store. Not used by default.

webapp.opendj2.ldap.truststore.password=. The trust store password. If you set up and configure a trust store, then you need to set this. Not used by default.

webapp.opendj2.ldap.isactivedirectory=. Designate whether Active Directory is used. true or false

webapp.opendj2.ldap.domains=. An optional, comma-delimited list of valid domains.

webapp.opendj2.ldap.description=. A description of the OpenDJ Instance.

- 4 Update your environment. To run only the specific steps related to multiple LDAP services, enter

```
> yab webapp-opendj2-update
```

```
> yab ldapinstance-opendj2-create
```

To update your entire environment, enter

```
> yab update
```

Review and Update Directory to QAD Database Mappings

During user synchronization, QAD Enterprise Edition makes a DSML search request and then receives a DSML search response.

The attributes and values returned in the DSML response typically do not match the fields in the user table associated with the application. For each QAD application, an attribute mapping file, `user-map.xml`, contains a list of attribute-to-field mappings, default values, and processing instructions. This file must be configured to manage the attribute mappings.

Each QAD application performing user synchronization requires a customized attribute mapping file (`user-map.xml`). The file must be customized based on what the particular QAD application requires to provision a user.

Planning is required so that the values in the customized attribute mapping file match what is expected by the QAD application. For example, in QAD Enterprise Edition, active users must have an active user reason code assigned. The reason codes themselves must first be defined using Reason Codes Maintenance (36.2.17).

Mapping between the LDAP directory attributes and the QAD database records is defined in the `user-map.xml` file. Reviewing the `user-map.xml` file requires some familiarity with LDAP attribute usage. You should review the directory using a tool such as Active Directory Explorer or JXplorer. You should also have some familiarity with QAD database tables as described in the [QAD Database Definitions Technical Reference](#).

The default `user-map.xml` file is located in a path such as:

```
.../build/catalog/packages/mfgcoreplus/n/n/n/qad.mfgcoreplus/config/user-map.xml
```

If you have trouble locating the file, enter:

```
./config/qad.mfgcoreplus/config/usre-map.xml
```

You must edit this file and define the attribute mappings that are needed based on how the Active Directory is organized.

XML Schema for user-map.xml

XML Schema for user-map.xml

Attribute name	Required	Default Value	Description
name	true	N/A	The Active Directory attribute name returned in the DSML response.
tableName	true	N/A	The table name mapping.
fieldName	true	N/A	The field name mapping.
overwrite	false	true	If true then the value is overwritten during an UPDATE of the user record. If false then the value is only written during the CREATE of the user record.
defaultValue	false	A2A	The default value to use if no value is provided in the DSML response.
filter	false	true	Remove attributes that do not match a mapping key. Useful for filtering multiple values such as the attribute <code>memberOf</code> .

Map Element Attributes

Zero or many map elements may be associated with an attribute. If no mapping elements are present, the attribute value will not be replaced.

Map Element Attributes

Attribute name	Required	Description
key	true	The case insensitive mapping key that is used when matching an attribute value.
value	true	The mapping value that will replace the original value.

Example user-map.xml

```
<user>
  <attributes>
    <attribute name="c" tableName="usr_mstr" fieldName="usr_ctype_code" overwrite="false">
      <map key="U.S.A" value="US" />
      <map key="AU" value="AUS" />
    </attribute>
    <attribute name="mail" tableName="usr_mstr" fieldName="usr_mail_address" overwrite="true" />
    <attribute name="c" tableName="usr_mstr" fieldName="usr_lang" defaultValue="US" overwrite="false">
      <map key="U.S.A" value="US" />
      <map key="AU" value="US" />
      <map key="DE" value="GR" />
    </attribute>
  </attributes>
</user>
```

The above user-map.xml file is summarized in the following table.

Active Directory Attribute	Table and Field	Default Value	Is Mapped	Overwrite
c	usr_mstr.usr_ctype_code	N/A	yes	yes
c	usr_mstr.usr_lang	US	yes	no
mail	usr_mstr.usr_mail_address	N/A	no	yes

LDAP Attribute Listing

Attribute Name	Alias	Description	Multiple Values	Syntax
c	countryName	Country abbreviation	false	DirectoryString
cn	commonName	Name	false	DirectoryString
co	friendlyCountryName	Full name of country	false	DirectoryString
codePage	codePage	Code page	false	Integer
countryCode	countryCode	Country code	false	Integer
dn	distinguishedName	X500 distinguished name	false	DN
displayName	displayName	Display Name	false	DN
gn	givenName	First or given name	false	DirectoryString
homePhone	homeTelephoneNumber	Home phone number	false	DirectoryString
mail	rfc822Mailbox	E-mail address	false	DirectoryString
memberOf	memberOf	Group membership	true	DN
mobile	mobileTelephoneNumber	Mobile phone number	false	DirectoryString
modifyTimestamp	mnodifyTimestamp	Modify time stamp	false	Generalized Time
o	organizationName	Organization name	true	DirectoryString
objectCategory		Object category	false	DN
ou	organizationalUnitName	Usually department or sub-entity	true	DNWithBinary
postalCode	postalCode	Post code or ZIP	false	DirectoryString

Attribute Name	Alias	Description	Multiple Values	Syntax
sn	surname	Surname or last name	false	DirectoryString
st	stateOrProvinceName	State	false	DirectoryString
street	streetAddress	Street address	false	DirectoryString
uid	userid	Username	false	DirectoryString

Syntax

Attribute Name	Format	Description	Example
Generalized Time	YYMMDDHHMMSS[.fraction][(+ -HHMM)Z]	Time stamp	"19991106210627.3Z" = Nov 6, 1999 21:06:27.3 UTC
DN	cn=<value>,ou=<value>,o=<value>,c=<value>	Distinguished name. Comma delimited list of name/value pairs (RFC 2253)	cn=Ben Gray,ou=editing,o=New York Times,c=US
DirectoryString		UTF-8 encoded string	QAD Inc.
Integer		Whole number of unlimited magnitude	12345

Once the attribute mapping in `user-map.xml` is complete, you can proceed with configuring QAD Enterprise Edition.

Download QAD .NET UI

Download and open the QAD .NET UI client from the home server URL.

Verify that the system is working. Open a program (such as Sales Order Maintenance [7.1.1]), a browse (such as Browse Master Browse [36.4.8.14]), and a Financials function (such as Role Membership Maintain [36.3.6.6]).

Configure SYNC reason code

- 1 Open Reason Codes Maintenance (36.2.17).
- 2 Set the following fields:
 - Reason Type: USER_ACT
 - Reason Code: SYNC
- 3 Click Next.

Configure Alternate Country Code

Depending on the data you have, Alternate Country Code might not be set, which can cause problems when you try to add a user. For each country where you have users, add an Alternate Country Code using Country Code Data Maintenance (2.14.1).

For example, for a US user, open Country Code Data Maintenance, set Country Code and Alternate Country Code to US, click Active on, and then click Next.

Configure LDAP Instance

Use LDAP Instance Maintenance (36.3.10) to configure LDAP.

- 1 In the QAD .NET UI, open LDAP Instance Maintenance and review the following fields:

LDAP Instance Name. opendj

Description. OpenDJ Instance or another appropriate description.

LDAP Servlet URL. http://domain:port/opendj/DSMLServlet, where domain is the Tomcat server.

LDAP Domains. Leave blank.

Is Active Directory. Select the check box if you are using Active Directory.

- 2 Click Next to save.

Verify LDAP Instance Definition for DSML Gateway Using User Sync

Note You should have your LDAP/Active Directory administrator present when connecting to the authentication server during initial setup and configuration.

The YAB console configures the DSML gateway instance for you in QAD Enterprise Edition. You can verify the configuration by testing one user.

Use User Maintenance (36.3.1) to sync one user at a time. This method is useful for debugging your connection methodology before starting batch imports, updates, or deletes.

- 1 Select the user you want to sync.
- 2 Select Next until the Active Directory fields are enabled at the bottom of the screen.

Fig. 4.1
User Maintenance

- 3 Select the Active Directory Enabled check box.
- 4 Enter the LDAP Instance Name; for example, `opendj`
- 5 Enter the Active Directory Username. This does not have to match the user name that is used to sign in to QAD Enterprise Edition.
- 6 Enter the LDAP Distinguished Name. This is the path that is used by your LDAP compatible product, such as Active Directory.

Note Active Directory requires you to escape special characters in an LDAP Distinguished Name. See documentation on Active Directory for details.

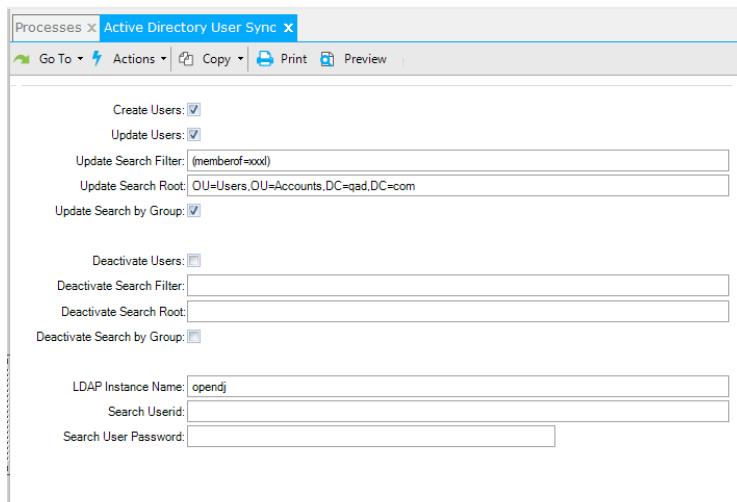
- 7 Click Next. If the sync completes successfully, the user record displays information from the LDAP server, which can include user details in the Remark field.
- 8 Check the `ldapsync-users.xml` and `ldapsync-exceptions.xml` log files for errors. These files are usually found in your working directory:
`./build/work/client/ldapsync-exceptions.update.xml/ldapsync-users.xml`
`./build/work/client/ldapsync-exceptions.update.xml/ldapsync-exceptions.xml`

Once you have successfully synced one user, you can use the LDAP Distinguished Name information in Active Directory User Sync (36.3.11) to create, update, or deactivate a single user or groups of users in QAD Enterprise Edition.

- Remove user information from the connection string.
- To update users, enter the remaining LDAP Distinguished Name information in the Update Search Root field.
- To deactivate users, enter the remaining LDAP Distinguished Name information in the Deactivate Search Root field.

The following example uses the `memberof` function to add multiple users at once. You must add users to a group to use this functionality. The Update Search Filter field identifies the group being added, while the Search UserID field identifies a user that can authenticate against the directory to get access to the directory data. The specifics for the Update Search Root and SearchUserID settings depend on your LDAP directory structure configuration.

Fig. 4.2
Active Directory User Sync



1 Open Active Directory User Sync (36.3.11), and set the following fields.

Note Use your memberof ID rather than xxx.

- Create Users: on
- Update Users: on
- Update Search Filter: (memberof=xxx)
- Update Search Root: OU=Users,OU=Accounts,DC=qad,DC=com
- Update Search by Group: off

Note Update Search by Group simulates the memberof function in Update Search Filter by running two queries. If your configuration supports memberof, do not select the Update Search by Group check box.

- Deactivate Users: off (and subsequent Deactivate-related fields are blank)
- LDAP Instance Name: (as specified in LDAP Instance Maintenance)
- Search UserID: domain\UserID
- Search User Password: (enter the password for the user specified in Search UserID)

2 Click Next.

Test LDAP

To verify your LDAP setup outside of Enterprise Edition, use a debugging tool such as JXplorer.

<http://www.jxplorer.org/>

API Authentication

QAD supports the following specifications for API authentication.

- HTTP Basic is the simplest way of enforcing access control to web resources by using the HTTP authentication header. Username and password information is sent as base-64 encoded text.

HTTP Basic is not recommended due to performance and security issues. Systems using HTTP Basic see significant performance degradation because credentials have to be reauthenticated with every request. Also, it presents security risks because authentication is done over unencrypted channels.

- OAuth2 provides a more secure way for REST API clients to authenticate users without sending user credentials with each request. The OAuth2 Specification requires a client to receive an access token and then pass the token to the resource sever as part of the request.

Users and Roles

This section describes how to set up users and roles in your system.

Overview 48

Describes role-based access control and its purpose.

Set Up Users 49

Illustrates how to set up users, define the different types of users, and specify access to domains and entities.

Set Up Roles 61

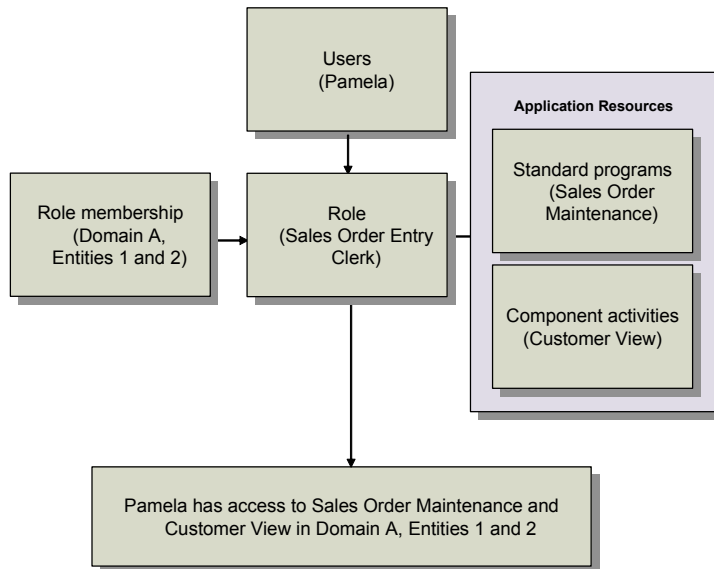
Explains how roles are used, how to define them and their permissions and memberships, how to export and import roles and permissions, and how to view access information for all types.

Overview

Role-based access control is a security mechanism that is designed to work with two basic user-defined elements: users and roles. Role-based access control limits users to executing only the system menu items belonging to their assigned role or roles.

Figure 5.1 illustrates the interaction of system users, role permissions, and role membership to determine the resources that are available to a user.

Fig. 5.1
Users and Roles

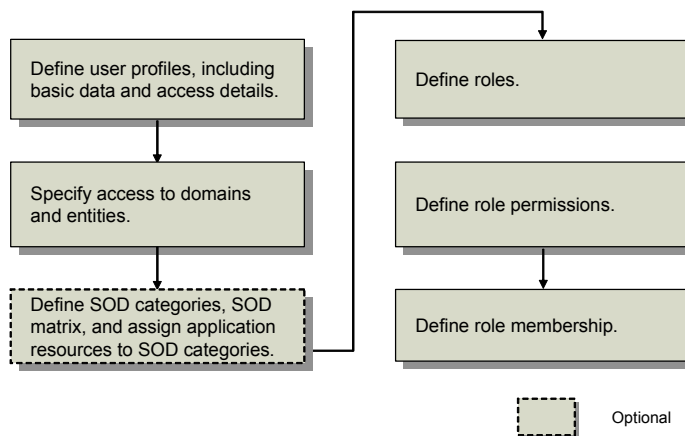


Role and User Definition Process Workflow

Before implementing your security model, you should develop a detailed security plan that describes how users and roles will be defined within your system to satisfy the business requirements of your organization. For details, see “Implementation Summary” on page 6.

Use the programs in the System Security Menu to set up and configure users and roles in your system. Figure 5.2 shows the user and role setup process workflow.

Fig. 5.2
Users and Roles Setup Flow



Note The overall flow used to set up users and roles is consistent between the QAD .NET UI and the Channel Islands UI. The following workflow contains information specific to the QAD .NET UI. For Channel Islands UI specific information, see “User and Role Workflow in Channel Islands” on page 74.

- 1 Create system users in User Maintenance (36.3.1), either manually, or automatically using LDAP for user synchronization. This step identifies each user to the system by providing them with a unique ID. You also provide basic user information to ensure that system data for each user is correctly displayed and processed, as well as specify security-related access settings and licensed applications. For details, see “Set Up Users” on page 49.
- 2 Specify user access to domains and entities in User Domain/Entity Access Maintain (36.3.4). For details, see “Specify Access to Domains and Entities” on page 59.
- 3 If you plan to implement segregation of duties, it is best to implement this internal control prior to defining roles and role permissions. Once associations between application resources and segregation of duties categories have been defined, role permission definitions are constrained by your segregation of duties policy. Implementing segregation of duties is optional. See Chapter 8, “Segregation of Duties,” on page 125.
- 4 Create roles in Role Create (36.3.6.1). All system users must be assigned to a role before they can access the system. For details, see “Set Up Roles” on page 61.
- 5 After creating user roles, define role permissions using Role Permissions Maintain (36.3.6.5). Role permissions determine which menu-level programs and activities a user can execute; they also determine a small number of non-menu level permissions. For details, see “Define Role Permissions” on page 67.
- 6 Then use Role Membership Maintain (36.3.6.6) to assign users to roles and specify the role context—that is, how the role operates within domains and entities. For details, see “Define Role Membership” on page 70.

Set Up Users

The process of setting up users identifies the users to the system and defines user-related information that the system requires. This process consists of:

- Defining users including:
 - Basic user information
 - Security settings
 - Application use
- Specifying the domains and entities each user can access

Users can be set up either manually or automatically using LDAP for user synchronization. Before proceeding, determine if you are defining users one by one through User Maintenance, or synchronizing user accounts using LDAP. If you are defining users one by one, continue with “Types of Users”. If you are synchronizing user accounts using LDAP, continue with “User Synchronization”.

User Synchronization

User synchronization is the process of synchronizing the user accounts of the multiple QAD applications with Directory Services, such as Active Directory or Open LDAP.

With user synchronization, QAD Enterprise Edition user accounts can be synchronized with a corporate LDAP directory (Active Directory). The configuration for user synchronization includes the use of a DSML (Directory Services Markup Language) gateway for LDAP communication between QAD Enterprise Edition and a corporate LDAP directory.

User and group synchronization allows you to simplify and securely manage information about users on multiple applications. Typically users are centrally managed on an identity management system, and access to applications is enabled through an application management portal. Centralizing the management of user information enables organizations to support the creation, management, and deactivation of users across multiple systems.

The user information in the Directory must be expanded to include information about which QAD applications a user is allowed to access. Each QAD application must have a unique identifier and the roles must correspond to the roles defined in the applications.

See Chapter 4, “Authentication,” on page 35 for details on setting up LDAP and “Verify LDAP Instance Definition for DSML Gateway Using User Sync” on page 43 for details on user synchronization.

Once users are synchronized, continue setting up users with “Specify Access to Domains and Entities” on page 59.

Types of Users

One of the fields that you specify when you create a user indicates the user type. Most users represent your company employees who perform day-to-day functions such as receiving purchased inventory, replenishing work centers, and filling sales orders.

However, the system also requires a number of users for performing background tasks that require system sign in. These users do not represent real individuals, and are typically given a user type of API (application program interface). Generally, this type of user should be associated with a role that grants full access to all domains, entities, and resources so that the required background tasks can be performed.

You specify these types of users in a number of different places:

- All of the daemon processes require a valid user ID and password for signing into the system. Typically you should create one user with access to all domains, entities, and resources and specify the same user for all the daemons. This makes administration simpler.
- System Maintain (36.24.3.2) requires a user ID and password for system startup activities that are initiated from the operating system or from a shortcut. This ID is used to establish that a valid user session can be created.
- A user role is defined during installation for QAD .NET UI administrative functions, that again needs access to all system resources.
- If you are using other components of QAD Enterprise Applications such as QAD Customer Self Service or QAD QXtend Inbound or Outbound, you need to configure a special user for interaction between the components.

Define Users

Use User Maintenance (36.3.1) to assign a unique ID to a system user and define related application and security details.

To access the system, each user must specify a unique user ID and the associated password. In addition each user must have been assigned a valid role and access to one or more domains and entities. Other user data is referenced throughout the system 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.

Once a user has accessed the system, the ID cannot be deleted. Instead, you can deactivate a user's record in the system. If an ID has never been used for sign in, you can delete it, if necessary. This lets you correct any errors made during initial setup. This restriction ensures a complete audit trail of users who have accessed the system.

Important The Active check box and the Enabled check box in User Maintenance have different functions.

- The Active check box controls whether a user's record is active within the system. Only active user records can be referenced when a new record is created in other system functions; in addition, lookups and browses only display active records.
- In contrast, the Enabled check box determines whether a user can sign in. By default, the Enabled check box is selected when a new user is created. A user can sign in to the system only if both the Enabled check box and Active check box are selected. The account of an active user can be disabled, for example, while they are on medical leave.

Note Any updates you make in User Maintenance are time stamped in Universal Time, Coordinated (UTC). For more information on the time stamping of transactions outside domains, see [QAD System Administration User Guide](#).

Fig. 5.3
User Maintenance (36.3.1)

User ID. Enter a code (maximum 8 characters) identifying a user in this database. This field cannot be blank or the same value as a role name. Do not use special characters, such as exclamation points (!) or commas (.). In addition, it is recommended not to use accented letters in user IDs. See Progress documentation for more information.

Note Progress does not recognize accented letters so it treats the accented and unaccented versions of, for example, the name Rene as the same user ID. However, the QAD .NET UI treats the accented and unaccented versions of the name as two different users. Therefore, favorite information related to the Rene account will not display for an accented version of the same name (user ID).

To sign in to the system, the user must supply a valid user ID.

If you plan to use OS-based security, the user IDs you create should be the same as the IDs defined for operating system sign in. See “OS-Based Sign-in Security” on page 20.

Depending on the setting of Header Display Mode in Security Control (36.24), the system may display this value on every program screen in the character interface. In the QAD .NET UI, the user ID always displays in the bottom message area. See “Header Display Mode” on page 27.

User Name. Enter a user name (maximum 35 characters) identifying the full user name associated with this ID.

The user name does not affect system security. It displays for reference on various reports and inquiries. To display an information window that includes the user name, press Ctrl+F from any program screen in the character interface.

Define Basic User Information

Defining basic information about system users includes setting options and defining values for:

- Controlling information process and display
- Identifying users
- Specifying e-mail addresses
- Enabling menu substitutions

Control Information Process and Display

You can ensure that system data is correctly displayed and processed for a given user—regardless of the user’s language or location—by specifying values for the Language and Country Code fields in User Maintenance.

Fig. 5.4
User Maintenance, Language and Country Code

The screenshot shows a web application window titled 'User Maintenance'. At the top, there are tabs for 'Processes' and 'User Maintenance'. Below the tabs is a toolbar with icons for 'Go To', 'Actions', 'Copy', 'Print', 'Preview', and 'Attach'. The main content area displays user information: 'User ID: janie' and 'User Name: Holly McKinnon'. Below this, there are two rows of input fields. The first row has 'Language: US' (with a dropdown arrow) and 'Variant: ' (with an empty text box). The second row has 'Country Code: US' (with a dropdown arrow) and 'Restricted: ' (with a checkbox).

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 signs in.

The language must be active and must be installed. Since labels, menus, messages, comments, and field help text are stored and retrieved by language code, you cannot assign a language to a user when these elements have not been loaded. Loading translated data automatically sets the associated language to installed.

Changes to this field do not affect any users currently signed in. Changes take effect only when they sign in again.

Country Code. Enter a valid, active country code defined in Country Create (36.1.3.1.1). The country code also must have an associated alternate country code defined in Country Code Data Maintenance (2.14.1).

The alternate country code must be a valid International Standards Organization (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.

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. See the installation guide for more information.

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 application 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

Fig. 5.5

User Maintenance, User Identity Fields

The screenshot shows a web form for user maintenance. The fields are arranged in two columns. The left column contains: 'User Type' (a dropdown menu with 'Employee' selected), 'Time Zone' (a dropdown menu with 'EST/EDT' selected), 'E-mail Def' (a dropdown menu), and 'E-mail Address' (a text input field). The right column contains: 'Access Location' (a dropdown menu with 'PRIMARY' selected), 'Initials' (a text input field), and 'Active' (a checkbox that is checked). Below these columns are two more fields: 'Menu Substitution' (a small icon button) and 'Remark' (a text input field).

Use the following fields to identify this user:

User Type. Specify 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 the system through an application programming interface connection or who represent background processes such as daemons.

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 might 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 (36.4.2) 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).

The time zone defaults from the Time Zone field of the domain you are signed in to when you create the user.

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`. The system 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.

Initials. Enter initials for the user (maximum 20 characters). Initials can be used in references and when performing searches.

Active. Indicate if this is an active record.

When a record is active, it can be referenced from other maintenance functions. When a record is inactive, it cannot be referenced when a new record is created in other functions. Inactive records are not included in lookups of valid values. However, marking a record as inactive does not prevent you from continuing to use existing records that reference the inactive value. In addition, inactive values display on reports.

Once a user ID has been used for sign in, it cannot be deleted from the system. If an ID is no longer needed, deactivate it.

The system automatically selects this check box for new users.

Remark. 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 disabled.

Specify E-Mail Addresses

Associate a valid e-mail address and definition with each user who receives system-generated messages by entering values into the E-Mail Address and E-Mail Def fields. When selected, the E-mail Address Login field enables users to sign in using their e-mail address.

E-mail can be used with many system features. For example:

- System administrators can receive automatic notification when user IDs are disabled because of sign 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.

- Various internal control features, such as segregation of duties and e-signatures, use e-mail to inform administrators of unusual system events.

Enable Menu Substitutions

Select the Menu Substitution check box to indicate whether menu substitution is enabled for individual users when employing the character interface. When menu substitution is enabled, inquiries display instead of browses. This setting has no effect when using the QAD .NET UI or the Channel Islands UI.

Enable Active Directory Access

The Active Directory section enables you to specify sign-in information for Active Directory.

Active Directory Enabled. Select this field to enable the user to sign in through Active Directory.

LDAP Instance Name. Enter the service name of the LDAP instance. The LDAP instance Name comes from settings defined in LDAP Instance Maintenance (36.3.10).

Active Directory Username. Enter the Active Directory username for this user.

LDAP Distinguished Name. Enter the LDAP distinguished name. A distinguished name is a sequence of relative distinguished names connected by commas.

Specify Security Settings

Use the System Access frame in User Maintenance to specify security-related access settings for each user.

Fig. 5.6
User Maintenance, System Access Frame

System Access

Enabled: ☒ Last Logon: 1/19/2018 04:37 EST/EDT

Enabled Reason: QAD_def QAD DEFINITION

Force Password Change: ☐

Update Password: ☐ Last Password Change: 11/7/2017

Delete Back Next

Enabled. Select the check box to indicate that this user ID can be used to sign in to the system. To disable an existing user ID, clear the check box.

The Enabled check box has a different function than the Active check box. The Enabled check box controls the ability of a user to sign in to the system. In contrast, the Active check box controls whether a user's record is active within the system.

Note Any time this check box is updated, the Enabled Reason field must also be updated.

Enabled is updated in the following ways:

- Automatically when you enter a new user ID. By default, the system selects the Enabled check box; you must manually enter an enabled reason.
- Automatically when the system disables an account for too many failed sign-in attempts. Enabled Reason is set to the code specified in Security Control. See "Maximum Access Failures" on page 28.
- Manually when you update an existing ID; for example, you can do this to re-enable a user that was previously disabled, or to disable an account when a user leaves the organization. You must enter an enabled reason.

Enabled Reason. Enter a reason code that indicates the reason for modifying the setting of Enabled. This reason code must be associated with reason type USER_ACT. See "Enabled Reason Type" on page 29.

You must update this field anytime you change the Enabled field.

Force Password Change. Indicate whether the system should force this user to create and validate a new password the next time he or she signs in to the system using the current password.

By default, the system selects this check box for new users and the check box cannot be updated. This lets you assign temporary, single-use passwords either automatically or manually.

By default, the system clears this check box for existing users unless the password has been changed. In that case, it is automatically selected and you cannot update it. This forces users to assign their own passwords at the next sign in.

Use Force Password Change Utility (36.3.23.12) to select this check box for users belonging to selected roles.

Note Any updates made using the Force Password Change Utility are time stamped in Universal Time, Coordinated (UTC). For more information on the time stamping of transactions outside domains, see [QAD System Administration User Guide](#).

Update Password. Specify whether this user requires a new password. For new users, the system selects this check box by default, and you cannot change it.

Update Passwords

When the Update Password check box is selected 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 sign in, the user is prompted to enter a new password.

Fig. 5.7
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 sign in, give them access to User Password Maintenance (36.3.3). See “Expiration Days” on page 31.

Specify Application Use

QAD applications support a number of license types. If you are using named user licensing, a finite set of users is predefined.

When the user count exceeds the number of licensed users, a violation message displays here. Violation messages can be either warnings or errors, depending on whether enforcement of the license policy is implemented or not. This is determined by the setting of Enforce Licensed User Count field in Security Control. See “Enforce Licensed User Count” on page 27.

- When Enforce Licensed User Count is Yes, an error displays and you cannot add new users when user count exceeds the number of licensed named users.
- When Enforce Licensed User Count is No, a warning displays and a violation is recorded, but system administrators can add new users.

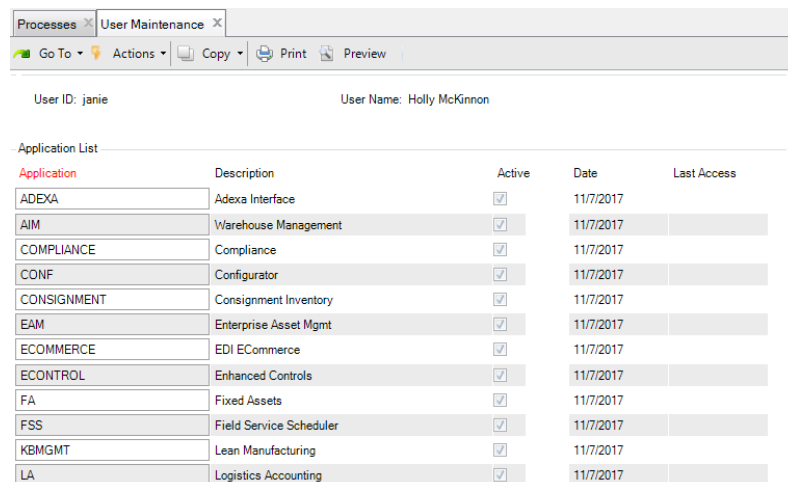
Important After you receive a warning, you can continue with software use. If you receive repeated warnings, contact your QAD sales representative or distributor for a license upgrade.

The applications that a user can access must be activated for the user; otherwise, the user cannot access the application. You can activate access to applications here, or when you register an application license code in License Registration (36.16.10.1).

Once a user has accessed the system, the ID cannot be deleted. Instead, you can make users inactive for an application. If an ID has never been used for sign in, you can delete it, if necessary. This lets you correct any errors made during initial setup.

Use the Application List frame in User Maintenance to define the software applications that a user can access. When you define a new user, the system prompts you to authorize the new user for all licensed applications. If you select the check box, the Active check box is selected for all licensed applications for this user. Otherwise, Enterprise Applications (MFG/PRO) is listed as the only active application. You can list additional licensed software applications, then select (or clear) the Active check box for each application. By default the check box is selected.

Fig. 5.8
User Maintenance, Application List Frame



Application	Description	Active	Date	Last Access
ADEXA	Adexa Interface	☒	11/7/2017	
AIM	Warehouse Management	☒	11/7/2017	
COMPLIANCE	Compliance	☒	11/7/2017	
CONF	Configurator	☒	11/7/2017	
CONSIGNMENT	Consignment Inventory	☒	11/7/2017	
EAM	Enterprise Asset Mgmt	☒	11/7/2017	
ECOMMERCE	EDI ECommerce	☒	11/7/2017	
ECONTROL	Enhanced Controls	☒	11/7/2017	
FA	Fixed Assets	☒	11/7/2017	
FSS	Field Service Scheduler	☒	11/7/2017	
KBMGMT	Lean Manufacturing	☒	11/7/2017	
LA	Logistics Accounting	☒	11/7/2017	

The application name you enter under Application Name must be registered with the system through License Registration (36.16.10.1). If not, an error message displays.

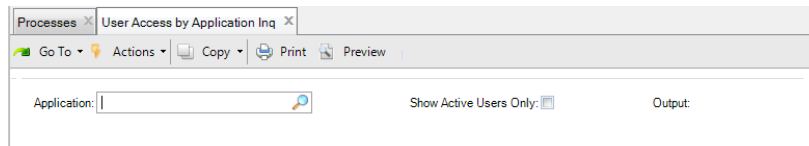
The system counts the number of enabled users authorized to access the application and compares the number against a predefined limit for your license type. If the number of enabled users exceeds the predefined limit, a violation message displays and you cannot add the application to the list.

You also can specify which users can access an application after you register the application in License Registration.

If you disable the Enterprise Application (MFG/PRO) setting for a user, all other registered applications are also disabled.

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. 5.9
User Access by Application Inquiry (36.3.23.4)



Specify Access to Domains and Entities

Use User Domain/Entity Access Maintain (36.3.4) to create or maintain user access privileges for domains and entities. The combination of domain and entity represents a workspace in the QAD .NET UI.

If you specify more than one domain, identify the default domain that the system should display at sign in.

To view access privileges for domains and entities, use User Domain/Entity Access View (36.3.5).

Function Overview

You must always define access to a combination of domain and entity. However, the entity dimension applies largely to financial data; most operational functions do not directly update data that is maintained at the entity level. When you are setting up users in a domain with multiple entities and these users will be working exclusively in operational areas such as manufacturing, sales, or service, assign them to the primary entity.

Be aware, however, that certain operational functions such as Operational Transaction Post (25.13.7) and Invoice Post and Print (7.13.4) do update entity-specific data. In these programs, access security defined in User Domain/Entity Access Maintain determines which entities can be updated.

Note The level of security access enforced—either domain or entity—displays in Role Permissions Maintain next to each menu item.

Domains and entities are defined as part of the process of setting up your foundation data. For more information on this topic, see [QAD Financials User Guide](#).

New domains and entities that are added to the system after implementation display in User Domain/Entity Access Maintain. You must explicitly grant users access before any updates can be made in the new domain.

Any changes to a user's domain or entity access privileges automatically update that user's role membership information. For example, removing a user's ability to access an entity breaks the association between that entity and the user's assigned role, and the entity is deleted from the list of assigned entities in Role Membership Maintain (36.3.6.6.1). For details on role membership see "Define Role Membership" on page 70.

Assign Access

User Domain/Entity Access Maintain provides a workbench type screen for streamlining the setup of access. You can use the three selection criteria fields to limit the records you want to work with or leave them blank to see all combinations in the system. The grid supports standard sorting and group-by features so you can organize the data conveniently.

Selecting a check box in the Select column indicates that the user has access to the associated combination of domain and entity.

Fig. 5.10
User Domain/Entity Access Maintain

Link	User Login	Domain Code	Default Domain	Entity Code	Primary Entity	Active Entity
☒	janie	QAD	☒	999 - SYSADM	☒	☒
☒	janie	10USA	☒	10CORPCONS	☐	☒
☒	janie	10USA	☒	10USACO	☒	☒
☒	janie	11CAN	☐	11NACONS	☐	☒
☒	janie	11CAN	☐	11CANCO	☒	☒
☒	janie	12MEX	☐	12MEXCO	☒	☒
☒	janie	20FRA	☐	20FRACO	☒	☒
☒	janie	21NL	☐	21NLCO	☒	☒
☒	janie	22UK	☐	22EMEACONS	☐	☒
☒	janie	22UK	☐	22UKCO	☒	☒
☒	janie	30CHN	☐	30CHNCO	☒	☒
☒	janie	31AUS	☐	31APCONS	☐	☒
☒	janie	31AUS	☐	31AUSCO	☒	☒
☒	janie	21NL	☐	21ITCO	☐	☒
☒	janie	23GER	☐	23GERCO	☒	☒
☒	janie	40BRZ	☐	40BRZCO	☒	☒
☒	janie	90TRN	☐	90TRNCO	☒	☒
☒	janie	80TST	☐	80TSTCO	☒	☒

You can also modify the user's default domain by selecting the Default Domain check box. Selecting this for one entity in a domain activates the setting for all entities, since the setting applies domain wide.

Note The Primary Entity column is for reference only and cannot be modified here. The domain's primary entity is specified in the Domain Create activity.

Default. Select the check box on the row of the user's default domain. Only one domain can be designated as default. In the QAD .NET UI, the default domain displays only on the first sign in; on subsequent sign ins the state of the last session displays.

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 signs in to the database, the system retrieves the information associated with the user's ID. In the character interface, 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 sign in but is automatically signed in to the single domain associated with the ID specified.

Users employing the QAD .NET UI can switch entities by opening a different workspace.

Set Up Roles

Roles are used to model the business processes that exist within a business enterprise. Roles determine the set of application resources that display for users when they access their permitted workspaces. In order to model your organization's business processes effectively, users need access to all the appropriate application resources required for them to perform their everyday business tasks.

In this context, an application resource typically is an executable program that exists within the menu system: either a standard program or a component-based activity. However, in addition to functions executed from the menu, some activities that are not on the menu can be secured.

All system users must be assigned to at least one role in order to gain access to the system. Typically the same role is given to more than one user in an organization, and a single user may have several assigned roles.

Note A user assigned to multiple roles has access to the combination of resources defined in the roles.

Role-based access control provides flexibility and consistency in the way security requirements are enforced, and also helps reduce maintenance for the system administrator. While your users may change based on terminations or task reassignments, roles within an organization typically remain stable over time.

Roles are not domain specific—they are defined system wide. However, roles operate within the context of the domains and entities to which the user has been granted access. This concept is known as *role membership*. See “Define Role Membership” on page 70.

Uses of Roles

The primary use of roles is to limit access to menu-level functions. Roles are also used to:

- Limit access to other resources such as sites and GL accounts. This is described in Chapter 7, “QAD .NET UI Security,” on page 99.
- Limit access to a set of activities that are not on the menu related to component-based functions.
- Create customized versions of component functions that are stored and retrieved at the role level.
- Create saved browse settings and report variants that are stored and retrieved at the role level.

The last two activities are described in *QAD System Administration User Guide* and *Introduction to QAD Enterprise Applications User Guide*.

Note The Process Maps display on the menu in the QAD .NET UI, but are not secured through role permissions. Anyone can view the maps. However, security is invoked when a user clicks a link in the process map that executes a menu-level program. If the user does not have access, an error displays.

Default Roles

Each user can be assigned a default role in Role Membership Maintain. This default is not related to security. For security, a user is granted the sum of resources assigned to the various roles assigned to them. However, for customizations, searches, and report variants saved at the role level, a default role is required to determine what to display.

Example Customized versions of Supplier Invoice Create are developed for role SalesClerk and SalesManager. The operations manager is assigned both of these roles, but SalesManager is marked as the default role. When the operations manager uses Supplier Invoice Create, the version customized for SalesManager displays.

If a user is not assigned a default role when multiple role-specific customizations exist, the system-level version of the function or report displays.

Non-Menu Resources

Most resources assigned to a role represent menu-level programs and activities. However, roles can be granted permission to a few system activities that are not on the menu.

Table 5.1 shows the activities that must be assigned permissions, but which do not appear on the application menu.

Table 5.1
Secured Items Not on Menu

Secured Item	Description
Customization – Design Mode General (Entity) Customization – Design Mode Role (Entity) Customization – Design Mode User (Entity)	Determines if users with this role can customize the user interface through the Design Mode features at the system, role, or user level. For details, see the section on design mode in QAD System Administration User Guide .
Supplier – Supplier Invoices (Entity)	Determines if users with this role can access the Supplier Invoices (for the current entity) Related View as a right-click option on Supplier browses.
Customer – Customer Invoice (Entity)	Determines if users with this role can access the Customer Invoices (for the current entity) Related View as a right-click option on Customer browses.
Customer – Customer Invoices Activity	Determines if users with this role can access the Customer Invoices Activity Related View as a right-click option on Customer browses.
Customer Invoice – Modify Due Date (Entity)	Determines if users with this role can modify invoice due dates using Customer Payment Selection Modify. Customer Payment Selection Modify is used in EDI Advanced Banking for Accounts Receivable. For details, see QAD Financials User Guide .

Secured Item	Description
Evaluated Receipt Settlement Create – (Entity) Evaluated Receipt Settlement Modify – (Entity)	Determines if users with this role can run the ERS Processor to generate supplier invoices and corresponding receiver matching records based on completed purchase order or fiscal receipts. For details, see QAD Financials User Guide .
ERS Line – Create (Entity)	Determines if users with this role can access the ERS logging activities run by the ERS Processor. You cannot run the ERS Processor if you do not have access to these activities.
General Ledger Masks – Maintain GL Masks (Entity)	GL masks have been replaced by COA masks. This option lets you access the old GL Mask Maintain function to verify the conversion to the newer COA mask functions.
Journal Entry – Create (External)	Determines if users with this role can create journal entries using an API. The API create method is used by both Operational Transaction Post (25.13.7) and Invoice Post and Print (7.13.4) to create journal entries. It could also be used to post transactions from an external system. You must assign this resource to any users that will be posting operational transactions to the GL.
Posting - Create External Posting (Entity)	Determines if users with this role can post transactions to external systems from the current entity during Operational Transaction Post (25.13.7).
Report Schedule – MaintainSchedule (Entity)	Determines if users with this role can maintain report schedules.
Report Variant Maintain on Role Level (Entity) Report Variant Maintain on System Level (Entity) Report Variant Maintain on User Level (Entity)	Determines if users with this role can save report variants at the role, system, or user level. For details, see QAD Financials User Guide .
Stored Search Maintain on Role Level (Entity) Stored Search Maintain on System Level (Entity) Stored Search Maintain on User Level (Entity)	Determines if users with this role can save stored searches at the role, system, or user level. For details, see Introduction to QAD Enterprise Applications User Guide .
User – Create (Entity) User – Delete (Entity)	Determines if users with this role can create or delete a user with User Maintenance (36.3.1). A role must have access to both User Maintenance and these two options to successfully create or delete a user. See “Define Users” on page 51.

Secured Item	Description
Tax Code – Create Tax Code – Modify Tax Code – Delete	Determines if users with this role can create, modify, or delete tax rates with Tax Rate Maintenance (29.4.1). A role must have access to both Tax Rate Maintenance and one of these options to successfully create, modify, or delete tax rates. Tax rates are described in the chapter on Global Tax Management in QAD Global Tax Management User Guide .
gencodegroup:APP (Domain) gencodegroup:SYSTEM (Domain)	Determines if users can modify generalized code fields belonging to these groups. If the administrator creates other generalized code groups, they are also displayed in this list. Generalized code groups are described in the chapter on Domain Constants in QAD System Administration User Guide .

System-Supplied Roles

During system installation, a number of roles are set up automatically. Table 5.2 lists these roles and their function.

Table 5.2
System Roles Created During Installation

Role	Description
_Everyone	This role is only present in systems that were converted from an earlier version of QAD software. It includes all users that were defined in the previous system.
CustomerNotify	Members of this role receive e-mail notification when a new customer record is created with Customer Create so that the operational data can be completed in Customer Data Maintenance (2.1.1).
EmployeeNotify	Members of this role receive e-mail notification when a new employee record is created with Employee Create so that the employee can be defined as a service/support engineer in Engineer Maintenance (11.13.1).
EndUserNotify	Members of this role receive e-mail notification when a new end user record is created with End User Create so that the operational data can be completed in End User Data Maintenance (11.9.1).
SuperUser	This role provides initial access to all menu functions and is typically assigned to users with an administrative role during system implementation.
SupplierNotify	Members of this role receive e-mail notification when a new supplier record is created with Supplier Create so that the operational data can be completed in Supplier Data Maintenance (2.3.1).

The SuperUser role is initially defined to provide permissions for all menu functions loaded in the system. However, this is true only initially. If you add new menu items manually using Menu System Maintenance (36.4.4.1), you must also manually grant users rights to these menu items in

Role Permissions Maintain. When you add new domains and entities, you must explicitly grant access to the SuperUser role for members of this role to continue to have access throughout the system.

Note This is important for certain roles that are used, for example, by daemon processes and require access to all system resources. See “Types of Users” on page 50.

You should define other system roles for special functions such as:

- An administrative role specified in Security Control (36.3.24) to receive e-mail notifications when specific security and controlled events occur.
- The QAD .NET UI includes some administrative functions that can be assigned to a specific role.

Role Example

A system administrator configures the system to control access to three functions based on each employee’s organizational level. Three types of access to financial functions are required: one for clerks, one for managers, and one for the CFO.

The system administrator creates three roles: *Clerk*, *Manager*, and *CFO*. Sara, the AP Clerk, is assigned to the Clerk role. Don, the AP Manager, is assigned to the Manager and Clerk roles. Jane, the CFO, is assigned all three roles. In this setup, illustrated in Figure 5.11, Jane’s roles grant her entry to all the levels she is authorized to access.

Fig. 5.11
Using Roles to Give Access

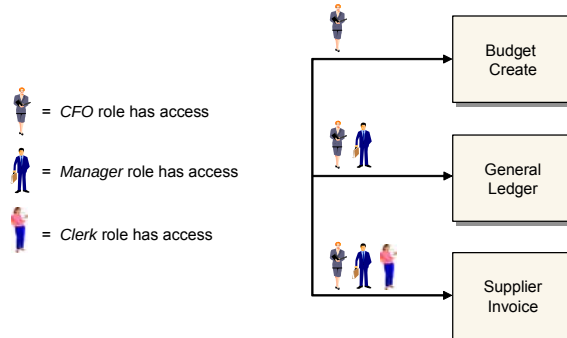


Table 5.3 shows how the system administrator assigns users to each role.

Table 5.3
Sample Role Setup

Role	User
<i>Clerk</i>	Sara, Don, Jane
<i>Manager</i>	Don, Jane
<i>CFO</i>	Jane

Next, the administrator uses Role Permissions Maintain to assign the appropriate system resources to the relevant roles to determine access to the system resources that each user requires in order to complete their assigned tasks.

When Mark is hired as the new deputy CFO, the system administrator only has to assign Mark to the *CFO* role in order to give him access to each individual protected financial function.

When a member of the SalesClerk role signs in, the user has access to:

- Sales Order Maintenance
- Customer View
- Customer Credit View

Instead of seeing the entire set of menus, only Customer Management and Financials display. Within these folders, only the selected functions SalesClerk can access display.

Note Using features of the QAD .NET UI, users can also create their own custom menu display under Favorites.

Define Roles

Use Role Create (36.3.6.1) to define roles in your system. You should define as many roles as required in order to model your business processes in the system. Use Role Modify (36.3.6.2) to perform maintenance on existing roles defined in your system, and Role View (36.3.6.3) to view roles.

A role defined in the system can be deleted using Role Delete (36.3.6.4) as long as the role is not referenced in the system.

Fig. 5.12
Role Create (36.3.6.1)

Name. Enter a name (maximum 20 characters) identifying a role. Names are restricted to the characters A–Z, a–z, and 0–9.

Note Superuser is an existing role and cannot be used as a name. This role is used during initial system setup and has access to all system functions.

Description. Enter a description (maximum 40 characters) of the role. You can optionally enter descriptions in more than one language. For more information on the Translation Option, see [Introduction to QAD Enterprise Applications User Guide](#).

Both the role name and description display in the lookup associated with role fields and on various reports and inquiries, as space permits.

Active. Indicate if this is an active record.

Although deactivated roles can still display within browses, a deactivated role cannot be selected from other system functions. If a role is deactivated, existing security records defined within the system that use the role are still valid and remain functional. However, no new security records that reference the deactivated role can be created—new role memberships or role permissions, for example.

Define Role Permissions

Use Role Permissions Maintain (36.3.6.5) to define the role permissions in your system. You define permissions for both resources on the menu and resources that are not on the menu.

For resources on the menu, note the following:

- Only executables can be secured, not folders. The folder represents a container to help logically organize functions, but no security is associated directly with it. If a user does not have access to any executable programs in a folder, that folder does not display on the menu.
- If an executable appears more than once in the menu tree, the same security always applies to it.

Example For user convenience, Maser Comment Maintenance (gpcmnts.p) appears on the menu as 1.12, 2.1.12, 2.3.12, 2.5.12, and 14.12. You cannot give a role access to menu 1.12 and not give them access to menu 2.1.12. The access is associated with gpcmnts.p, not the menu position. The menu numbers are used only to make it easier to logically group programs.

- Regardless of how a menu resource is accessed, the same security applies. For example, related functions can be accessed from a Go To menu only when the current user has access to the destination function. This is also true of the related views and reports; users must have access to the menu-level program to be able to run it from within another function.

Note When using an API to access the application, you must provide a sign in that has permissions for the activity you want to perform.

- When a new item is added manually in Menu System Maintenance (36.4.4.1), it is initially inaccessible to all users, and consequently, will not be seen on the menu. You must assign the menu to a role before members of that role can see or use the menu.

Important You should keep this in mind when customizing the menus; if you simply add the item to the menus and check to see if it appears, you will not be able to see it. You must add it to a role and be signed in as a user with that role to see the new menu.

- Menus are cached in memory during sign in; you must sign out and sign in again to see any menu changes. Changes to role permissions do not affect any users currently signed in. Changes take effect the next time they sign in. This approach avoids performance degradation from continually checking for security changes.

Note Lookups that let you select a record are not separately secured. Access to a function implies access to all lookups used in the function. When a lookup contains links to drill-down browses, these are only secured if they are on the menu. If a power-browse is not secured by being put on the menu, anyone can execute it.

Role-based permission prevents any executable from being run from within your QAD application unless it is added to the menu and then added to a role. You cannot directly invoke a Progress program that is not on the menu by typing its name at the menu prompt in the character user interface.

When users attempt to execute a program on the menu and their current role does not grant access, the message “Program not found” displays.

Important To access the program and field help in the QAD .NET UI, a user must have access to Field Help Maintenance (36.4.13). If a user is unable to access the help, a possible cause of the problem is that the user does not have access to Field Help Maintenance (36.4.13).

Figure 5.13 illustrates Role Permissions Maintain. You can define secured items on the menu and secured items not on the menu. Both top-level selections display application resources defined in the system using a tree model with leaf and non-leaf nodes, similar to how the menu itself displays.

Fig. 5.13
Role Permissions Maintain (36.3.6.5)

Secured Items on Menu

Each menu item displays identified by menu number and arranged according to the system menu. Any selected items represent the menu items currently assigned to the specified role. Each menu item corresponds to a record in the mnd_det table.

To assign a menu item to a role, open the relevant menu grouping, navigate to the menu item you want to associate with the selected role, and click in the check box next to the item.

Fig. 5.14
Role Permissions Maintain, Secured Items on Menu

Role Name:

Role Description:

Filter:

- ☐ Secured items on menu
 - ☐ Customer Management
 - ☐ Sales Orders/Invoices (7)
 - ☐ Configured Products (8)
 - ☐ Service/Support (11)
 - ☐ Customer Management Roles (75)
 - ☐ Supply Chain
 - ☐ Warehousing (4)
 - ☐ Purchasing (5)
 - ☐ Distribution Plan (12)
 - ☐ Product Line Plan (20)
 - ☐ Resource Plan (21)
 - ☐ Operations Plan (33)
 - ☐ EDI eCommerce (35)
 - ☐ Manufacturing
 - ☐ Product Structure (13)
 - ☐ Routings/Work Centers (14)
 - ☐ Formula/Process (15)
 - ☐ Work Orders (16)
 - ☐ Lean Manufacturing (17)
 - ☐ Repetitive (18)
 - ☐ Quality Management (19)
 - ☐ Financial Management (20)

The tree nodes can be expanded and contracted. Nodes can have one of three possible states:

- Clear. No selection is in effect.
- Gray check mark. One or more but not all of the leaf nodes or non-leaf nodes lower in the tree are selected.
- Black check mark. The top-level node and all lower level nodes are selected.

Selecting a node within a node causes the node higher up to display as shaded. Selecting a node causes all items below it to be selected and is indicated in the higher node. The ability to select a node and cause lower nodes to also be selected streamlines the process of setting permissions.

Since menu items on submenus inherit associations created at a higher level, you can associate a menu group high in the menu tree, clear any unwanted associations for submenus, and then modify selections at the menu item level, if required. This makes the process of administering role permissions easier.

Menu items in the tree display with [Domain] or [Entity] after the menu description. This indicates the level at which security access is checked when this function is executed. Most operational functions are secured at the domain level and most financial functions are secured at the entity level.

- When [Domain] displays, the function can be executed when the user has access to at least one entity within the domain.
- When [Entity] displays, the function can be executed only when the user has access for the specific entity.

Note Do not confuse this with the level of the data being updated by the function. For example, Tax Type Maintenance (29.1.1) is secured at the domain level, even though tax types can be used system wide.

Secured Items Not on Menu

Activities that can be secured even though they are not on the menu are displayed based on the component name and the activities associated with the component. Selected items are currently assigned to the specified role.

You assign items to a role in the same way you assign menu items, by clicking in the check box next to the item.

Fig. 5.15
Role Permissions Maintain, Secured Items Not on Menu

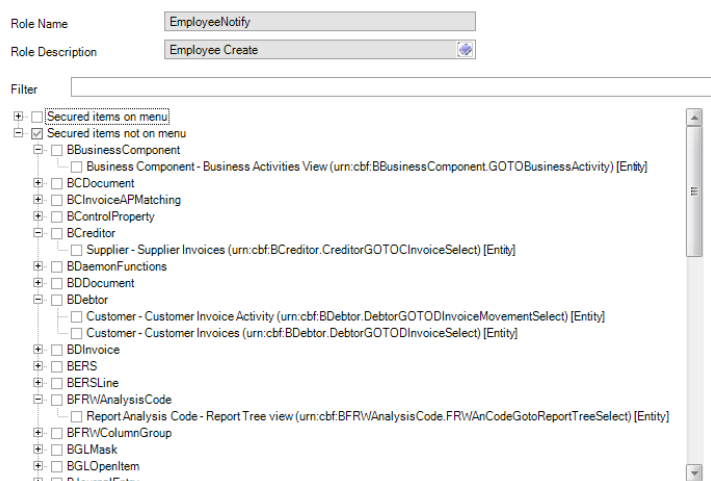


Table 5.1 on page 62 lists these functions and explains their use.

If you plan to let users customize screens for component-based functions to suit their working preferences, you must assign at least one of the Design Mode permissions to the user. If none of these permissions is assigned, the Design Mode menu option does not display on the Tools menu for that user. For details on customizing screens, see [QAD System Administration User Guide](#).

Define Role Membership

Use Role Membership Maintain (36.3.6.6) to define an association between a role defined in the system and a system user and to indicate which role is the user's default role. The default role does not affect security, but is used to determine role-specific customizations and stored searches. See "Default Roles" on page 62 for details.

The screen presents a workbench-type interface where you can select records to update by user, role, domain, and entity.

Note Although you can leave all fields blank when generating a list, this is not recommended since the list may take a long time to display, depending on the number of records in the database.

Role membership is always qualified by domain and entity. This is true even though for most operational functions, the specific entity is not relevant. To execute these operational functions, a user must still belong to a role that has access to at least one entity—typically the primary entity—in the domain.

Specifying role membership defines both who belongs to the role and the *role context*; that is, which domains and entities the role can access.

When a user signs in, the system builds the menu for that user by combining:

- All standard functions belonging to all roles assigned to the user in any entity of the selected domain
- All component activities belonging to all roles assigned to the user in the selected entity

Example Domain A has entities located in California, New York, and London. Carol has been assigned the role HR Manager for all three entities. Tom has been assigned the same role, but only for London; Pam and Tom share responsibilities for London. Pam's role membership is specified for entities California, New York, and London. Tom's role membership, however, is defined for the London entity only.

Fig. 5.16
Role Membership Maintain (36.3.6.6)

Link	User Name	Entity Code	Role Name	Default Role
☒	Holly McKinnon	10CORPCONS	SuperUser	☒
☒	Holly McKinnon	10CORPCONS	EmployeeNotify	☐
☒	Holly McKinnon	10CORPCONS	SupplierNotify	☐
☒	Holly McKinnon	10CORPCONS	CustomerNotify	☐
☒	Holly McKinnon	10CORPCONS	EndUserNotify	☐
☒	Holly McKinnon	10CORPCONS	qadadmin	☐
☒	Holly McKinnon	10CORPCONS	uidesign	☐
☒	Holly McKinnon	10CORPCONS	rptDsgn	☐
☒	Holly McKinnon	10CORPCONS	rptAdmin	☐
☒	Holly McKinnon	10CORPCONS	ProductTrxns	☐
☒	Holly McKinnon	10CORPCONS	ProductModify	☐
☒	Holly McKinnon	10CORPCONS	InventoryModify	☐
☒	Holly McKinnon	10CORPCONS	PostAutoBalNotify	☐
☒	Holly McKinnon	10USACO	SuperUser	☒
☒	Holly McKinnon	10USACO	EmployeeNotify	☐
☒	Holly McKinnon	10USACO	SupplierNotify	☐
☒	Holly McKinnon	10USACO	CustomerNotify	☐
☒	Holly McKinnon	10USACO	EndUserNotify	☐
☒	Holly McKinnon	10USACO	qadadmin	☐
☒	Holly McKinnon	10USACO	uidesign	☐
☒	Holly McKinnon	10USACO	rptDsgn	☐
☒	Holly McKinnon	10USACO	rptAdmin	☐
☒	Holly McKinnon	10USACO	ProductTrxns	☐
☒	Holly McKinnon	10USACO	ProductModify	☐
☒	Holly McKinnon	10USACO	InventoryModify	☐
☒	Holly McKinnon	10USACO	PostAutoBalNotify	☐

Use the User, Role, Domain, and Entity fields at the top of the screen to select the records you want to work with during this session. You can group the data in the grid or sort or rearrange columns to streamline the setup activity. Selecting the check box indicates that the user has access to the role for the associated domain and entity.

Note Any changes to a user's domain or entity access privileges also automatically update that user's role membership information. For example, removing a user's ability to access an entity breaks the association between that entity and the user's assigned role, and the entity is deleted from the list of assigned entities in Role Membership Maintain. For details on defining user access to domains and entities, see "Specify Access to Domains and Entities" on page 59.

View Access Information

The following view programs display security-related information:

- User Domain/Entity Access View displays access privileges that can be filtered on user, domain, and entity.
- Role Permissions View displays permissions filtered on resource or role.

- Role Membership View displays the combinations of role and user filtered by domain, entity, role, or user.
- User Access View is an overall view of all dimensions: user, role, entity, domain, and resource.

Export and Import Roles and Permissions

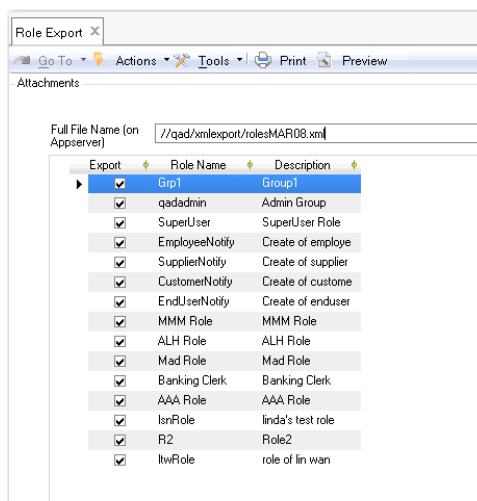
The default roles available in the system are loaded from the file `defaultroles.xml` during the initial install or as part of a system synchronization or update.

Use Role Export (36.3.6.11) and Role Import (36.3.6.12) to export and import roles, their descriptions, and permissions as `.xml` files. The function requires the full file name and location on the application server for the file to be exported or imported. The Import function uses synchronization logic to replace `defaultroles.xml` with the imported file.

The system displays an error message if the file name extension is incorrect, and a confirmation message when the export or import has completed successfully.

Role Export

Fig. 5.17
Role Export



The screenshot shows the 'Role Export' window. At the top, there is a 'Full File Name (on Appserver)' field containing the path `//qad/xmllexport/rolesMAR08.xml`. Below this is a table with columns 'Export', 'Role Name', and 'Description'. The 'Export' column contains checkboxes, all of which are checked. The 'Role Name' and 'Description' columns list various roles and their functions.

Export	Role Name	Description
☒	Grp1	Group1
☒	qadadmin	Admin Group
☒	SuperUser	SuperUser Role
☒	EmployeeNotify	Create of employee
☒	SupplierNotify	Create of supplier
☒	CustomerNotify	Create of custome
☒	EndUserNotify	Create of enduser
☒	MMM Role	MMM Role
☒	ALH Role	ALH Role
☒	Mad Role	Mad Role
☒	Banking Clerk	Banking Clerk
☒	AAA Role	AAA Role
☒	IsnRole	linda's test role
☒	R2	Role2
☒	ltwRole	role of lin wan

Full Filename (on Appserver). Specify a name and path for the exported file. You must use the `.xml` file extension.

Select the roles to be exported and click Export.

Channel Islands UI Security

This section applies only if you are using QAD Enterprise Edition with the Channel Islands UI. It covers the following topics:

Overview 74

Explains users, roles, and menus within the Channel Islands UI.

Prerequisites 74

Describes the prerequisites for Channel Islands.

User and Role Workflow in Channel Islands 74

Describes the ideal work flow for introducing users and roles into Channel Islands.

Resources 74

Explains Channel Islands resources and how to secure resources.

Users and Roles 75

Highlights how users and roles are created for Channel Islands.

Menus 76

Describes role and favorites menus and using menus to assign permissions to roles.

Role Permissions 80

Describes the Role Permissions screen and how to assign permissions to roles.

User Access 95

Explains how to define access to Channel Islands.

Configure Stored Views Access 97

Explains how to save customized screen layouts, emphasizing important information needed for everyday use and specific tasks.

Overview

Creating and maintaining a secure environment for the Channel Islands UI requires initial steps in the QAD .NET UI. Once these steps are complete, security can be maintained within the Channel Islands UI.

Prerequisites

You must be running Enterprise Edition with the Channel Islands UI.

User and Role Workflow in Channel Islands

- 1 Create system users in the QAD .NET UI in User Maintenance (36.3.1). See “Set Up Users” on page 49.
- 2 Create roles in the QAD .NET UI in Role Create (36.3.6.1). For details, see “Set Up Roles” on page 61.
- 3 Create role menus in Channel Islands for the newly created roles and assign permissions to those role menus. See “Create a New Role Menu” on page 76.
- 4 Specify user access to domains, entities, and sites in User Access. See “Set System Access” on page 95.
- 5 Assign users to roles in User Access. All Channel Islands users must be assigned to at least two roles, one of which is `webui_user`, before they can access the system. See “Assign Roles” on page 96.
- 6 Configure settings for stored views, which allow users to customize screen layout. See “Configure Stored Views Access” on page 97.

Resources

Channel Islands is made up of resources, which are uniquely identifiable pieces of the product that have been designated as needing to be secured. Securing resources limits access to specific roles that have been given adequate permission to interact with different areas of the system. All resources can be secured.

The security model in Channel Islands is more granular than the model in QAD .NET UI. Resources in Channel Islands range from the app level down to individual fields, unlike QAD .NET UI resources, which are typically executable programs and certain activities that do not appear on the menu.

Channel Islands Resources

The following resources can be secured in Channel Islands.

App. A collection of programs that express a cohesive set of business services through a well-defined interface. The set of exposed services defines a high-level area of business functionality.

Business Entity. The business logic and data necessary to represent real-world elements, such as sales orders, within the Channel Islands UI.

Browse. The QAD .NET UI, Progress-based “.p” browse programs that display data in a read-only browse table. You cannot edit or delete the existing data, nor add additional records to the browse table. You can filter the data.

View. A screen that organizes a toolbar, a grid with a list of records, and a form for completing work. Related fields and functions are grouped within panels, and a navigation bar provides access to panels.

Report. A view of data generated from multiple data sources based on a given filter criteria.

Service. The methods for each business entity as interface services, identified with the entity name and an “i” prefix in their URI. For example:

urn:service:com.qad.acme.generalizedcode.IGeneralizedCode for Generalized Code.

Dashboards and KPIs. Metrics used to create Action Centers. Dashboards are directly associated with users, unlike other resources that are associated with roles.

Field. A single element of data in a business entity.

Field Group. A logical grouping of fields that are part of a business entity and can be secured as a single entity.

Users and Roles

All Channel Islands users and roles must be set up in the QAD .NET UI. Users are set up through User Maintenance (36.3.1), and roles are defined in Role Create (36.3.6.1). For detailed information, see “Define Users” on page 51 and “Define Roles” on page 66.

After you create a role in the .NET UI, the role’s permissions should be configured through Role Permissions in the Channel Islands UI. See “Role Permissions” on page 80.

Note If you are creating a new role based on an existing role in Channel Islands, see “Role Menu” on page 76 for information on copying menu items and setting permissions.

Default Roles

Your system arrives with a variety of predefined, pre-configured roles. These roles are provided as starting points for the roles you will create for your system. You should not use the default roles, except for webui_user, for your users because any permission changes you make to the default roles will be overwritten with each software update. You can review the default roles’ associated permissions on the Role Permission screen and use these default settings as a guide when assigning permissions to new roles.

The default roles’ permissions are set using the principle of least privilege, which grants users access to only the resources they require to complete the roles’ tasks.

Note If you are creating a new role based on a default or existing role, see “Role Menu” on page 76 for information on copying menu items and setting permissions.

Menus

The Menus browse is a collection of all menus that exist in the Channel Islands environment. The browse displays all QAD-provided role menus, all non-QAD role menus, and all user favorites menus.

Menus are made up of menu-eligible resources, which are resources that have their own views and can be displayed in the Menu Bar. These resources can be grouped into folders, with the folder name appearing on the Menu Bar and the folder contents visible in the associated drop-down menu.

Users see the menus for the roles to which they have been granted access in the Channel Islands UI.

Role Menu

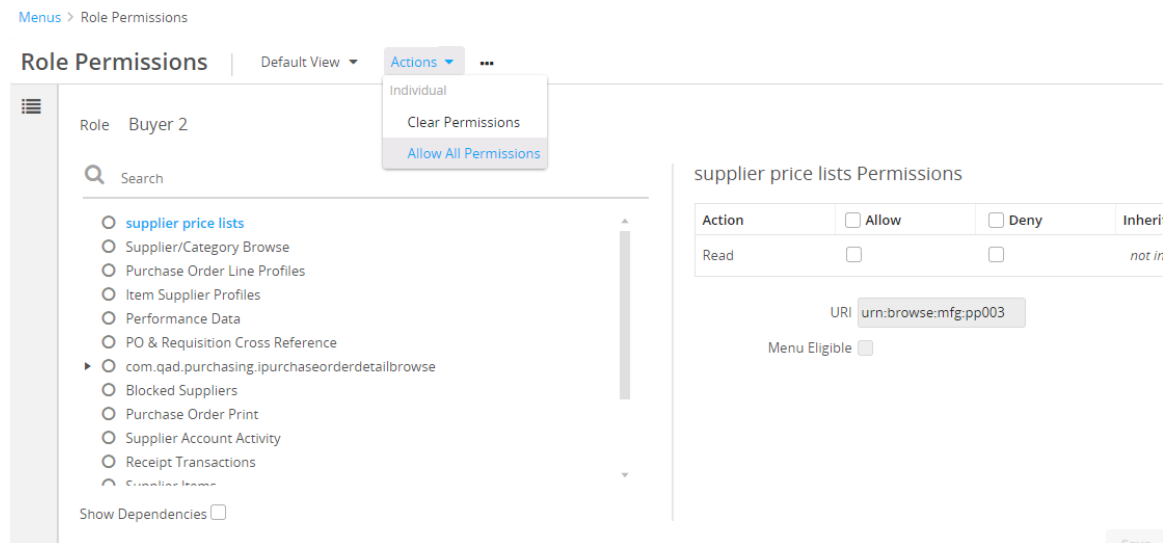
QAD-provided role menus cannot be modified or deleted but can be copied to create new role menus for roles. The new role menus can be edited and updated with additional folders, pages, and permissions. Role menus are selected through the Channel Islands menu bar and users see a role menu for each role to which they have been assigned that has a defined role menu.

Create a New Role Menu

Before you can create a new role menu, the system must have a role that is not yet associated with a role menu. To create a new role in the QAD .NET UI, see “Set Up Roles” on page 61.

- 1 Select New.
- 2 Select Role from the Type drop-down menu.
- 3 In the Name lookup, select the role to which to assign this role menu.
- 4 Save the role menu.
- 5 Add Pages and Folders to the new role menu. These folders and pages become the drop-down menus available in the menu bar for this role.
 - a Pages are the system’s menu items.
 - b Folders organize pages. Enter a new folder name or choose a label from the options in the system. If you select from the system-provided labels, the folder names will translate for users assigned different language codes.
- 6 Save the populated role menu.
- 7 Select Permissions at the bottom of the screen. The Role Permissions modal dialog displays the resources that make up the role menu you created. These resources need to be secured for the role to have access to all required areas of Channel Islands.

Fig. 6.1
Allow All Permissions



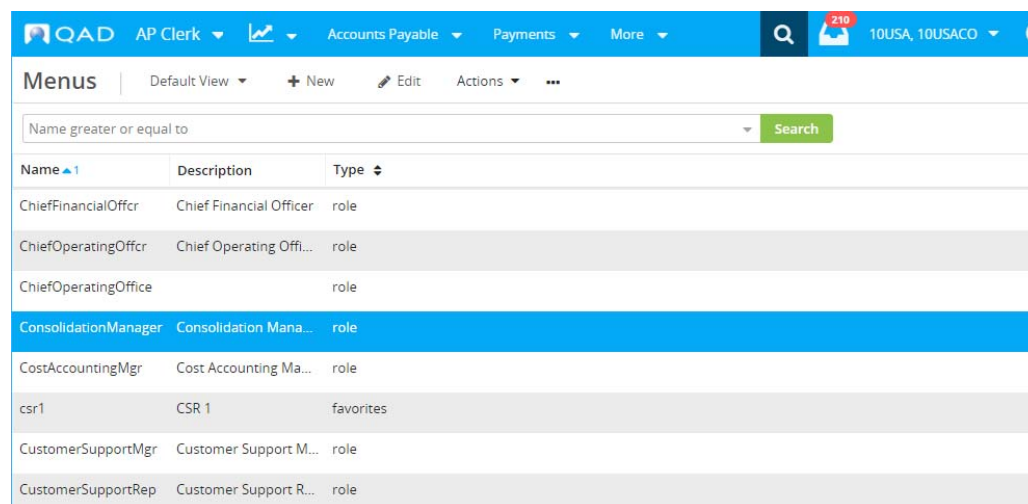
- 8 Select Allow All Permissions from the Actions menu.
- 9 All of the secured resources should now have a green circle next to them. Select Save in the lower right corner of the Role Permissions window.

Copy an Existing Role Menu to Create a New Role Menu

Before you can copy a role menu to create a new role menu, the system must have a role that is not yet associated with a role menu. To create a new role in the QAD .NET UI, see “Set Up Roles” on page 61.

- 1 On the Menus browse, highlight the role menu you want to copy.

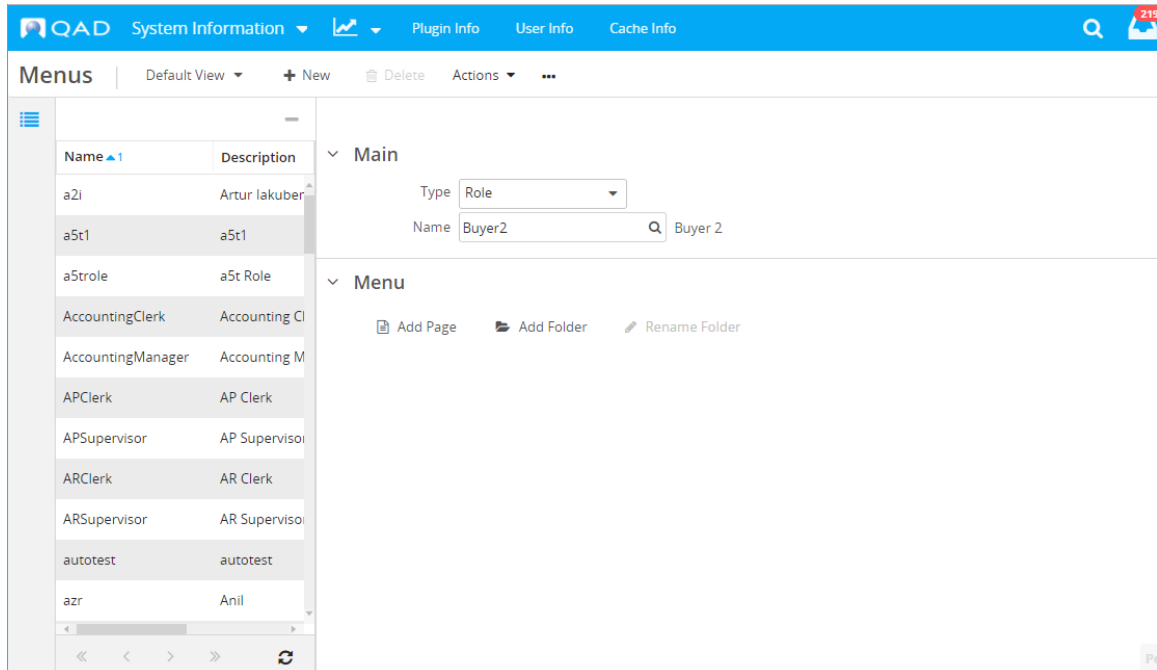
Fig. 6.2
Menus



- 2 Select Copy from the Actions menu.

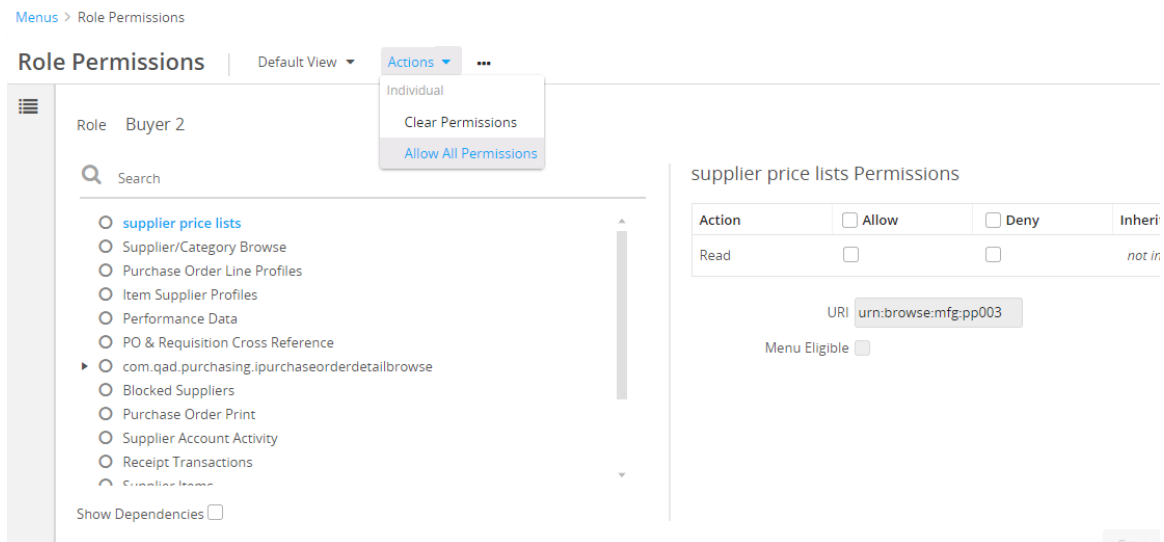
- 3 Select Role from the Type drop-down menu.
- 4 In the Name lookup, select the role that will be assigned this role menu.

Fig. 6.3
Copy a Role Menu



- 5 Select Save. Then select Permissions at the bottom of the screen. The Role Permissions modal dialog displays the resources that make up the role menu you copied. These resources need to be secured for the new role to have access to all required areas of Channel Islands.

Fig. 6.4
Allow All Permissions



- 6 Select Allow All Permissions from the Actions menu.

- 7 All of the secured resources should now have a green circle next to them. Select Save in the lower right corner of the Role Permissions window.

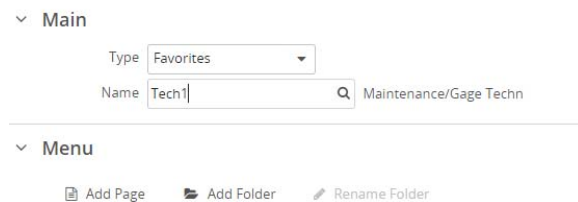
Favorites Menu

Favorites menus are not provided by QAD and can be updated by users and administrators; however, only administrators can configure Favorites menus from the Menus browse. Users can configure their own Favorites menu through the user drop-down in the menu bar.

Create a New Favorites Menu for a User

- 1 On the Menus browse, select New.
- 2 Select Favorites from the Type drop-down menu.
- 3 In the Name lookup, select the user ID to which to copy this role menu.

Fig. 6.5
Create New Favorites Menu



▼ Main

Type: Favorites

Name: Tech1 Maintenance/Gage Techn

▼ Menu

Add Page Add Folder Rename Folder

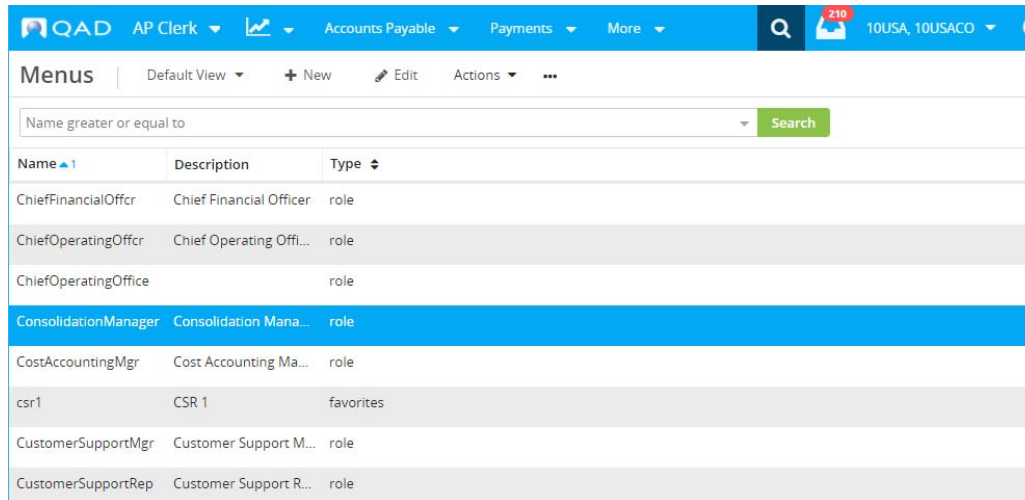
- 4 Add Pages and Folders to the new Favorites menu. These folders and pages become the drop-down menus available in the menu bar for this role.
 - a Pages are the system's menu items.
 - b Folders organize pages. Enter a new folder name or choose a label from the options in the system. If you select from the system-provided labels, the folder names will translate for users assigned different language codes.
- 5 Select Save.
- 6 Select Permissions to check that the user's role has adequate permission to access the newly assigned Favorites menu. If all resources are not green, you can choose Allow All Permissions from the Actions menu. but remember that you are updating the resources for the role, not just this user.

Copy a Menu to a User's Favorites Menu

You can use an existing menu as the basis of a user's Favorites menu. This action can only be done for a user that does not have a Favorites menu.

- 1 On the Menus browse, highlight the role menu you want to copy.

Fig. 6.6
Menus



Name	Description	Type
ChiefFinancialOffcr	Chief Financial Officer	role
ChiefOperatingOffcr	Chief Operating Offi...	role
ChiefOperatingOffice		role
ConsolidationManager	Consolidation Mana...	role
CostAccountingMgr	Cost Accounting Ma...	role
csr1	CSR 1	favorites
CustomerSupportMgr	Customer Support M...	role
CustomerSupportRep	Customer Support R...	role

- 2 Select Copy from the Actions menu.
- 3 Select Favorites from the Type drop-down menu.
- 4 In the Name lookup, select the user ID to which to copy this menu.
- 5 Select Save.

Note You cannot copy a Favorites menu to a user that already has a Favorites menu.

- 6 Select Permissions to check that the user's role has adequate permission to access the newly assigned Favorites menu. If all resources are not green, you can choose Allow All Permissions from the Actions menu, but remember that you are updating the resources for the role, not just this user.

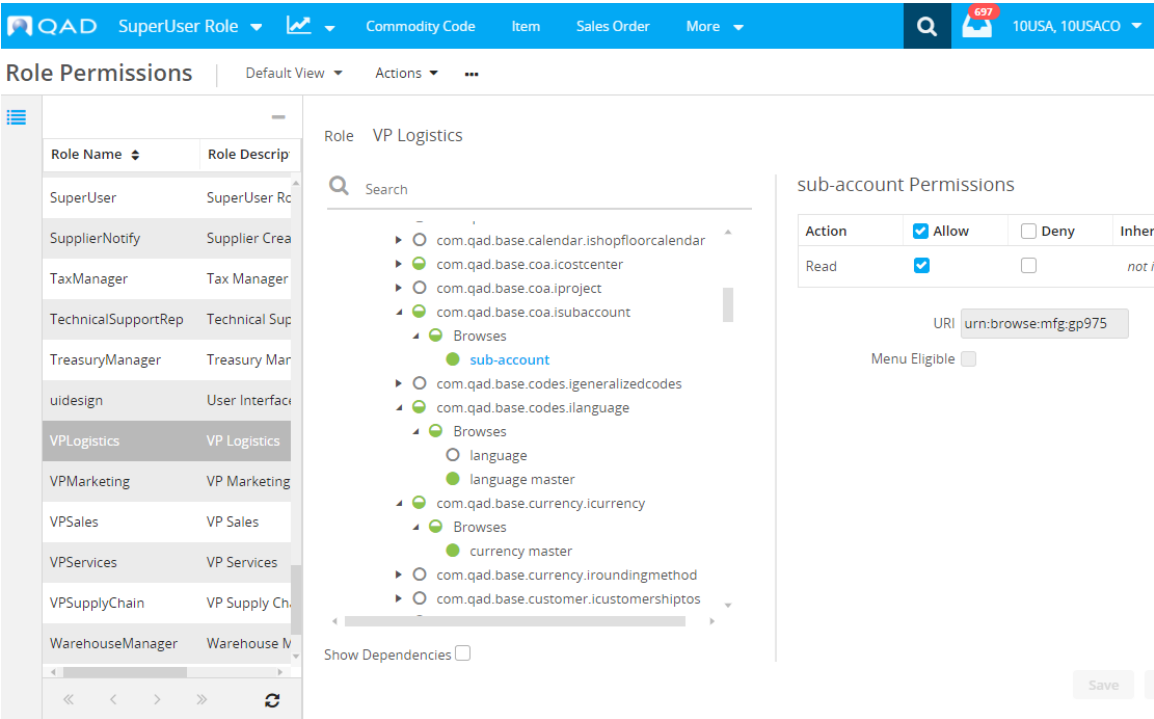
Role Permissions

Permissions for the Channel Islands UI should be set up and configured through the Channel Islands UI, though the task can be completed using the QAD .NET UI.

Note Use role menus to accurately and efficiently set permissions on new roles. See “Role Menu” on page 76 for more information.

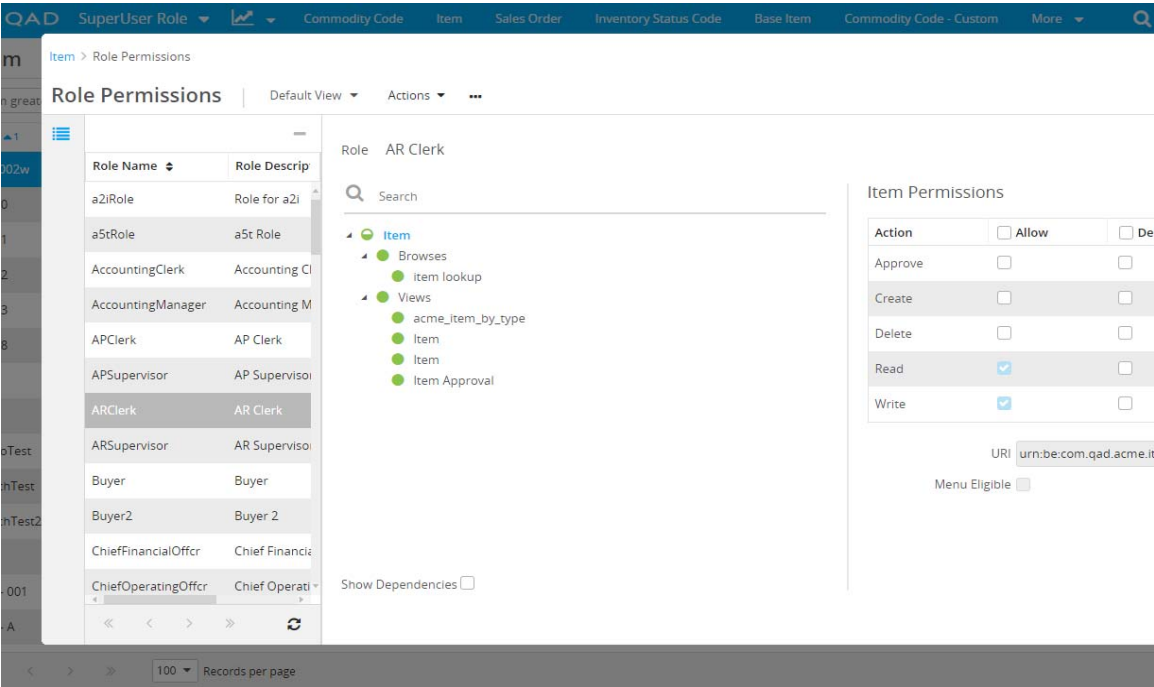
Role permissions information can be accessed through the main Role Permissions screen or as a modal dialog by selecting Permissions from the ellipses icon on every screen in the Channel Islands UI. The main Role Permissions screen, shown in Figure 6.7, displays of all the resources that can be secured in the system.

Fig. 6.7
Role Permissions



By contrast, far fewer resources are available to secure in the Permissions Tree when you select Permissions from the ellipses icon on an individual screen, such as the Item browse in Figure 6.8. The Role Permissions modal dialog shows only the resources associated with that screen, which allows you to do more granular editing for the roles that require access to the screen.

Fig. 6.8
Item Permissions



Permissions Inheritance and Configuration

Permissions are assigned in a top-down manner, with automatic inheritance for child resources. When you grant Allow access to a parent resource, all children of that resource are granted full permission. You can manage the granularity of child permissions, such as specific lookup tables, by setting those permissions to Deny. If, however, you deny access to a parent resource, all children of that resource are denied access, regardless of what their individual settings are. You cannot set the permission of a child resource to Allow if any permission further up the menu tree has been set to Deny.

Note For security reasons, grant access to the minimum permissions a role needs to complete required tasks.

Permissions Table

Every resource has an associated permissions table, which displays to the right of the permissions tree when you select a resource in the tree.

Fig. 6.9
Permissions Table

Business Entities Permissions

Action	☒ Allow	☐ Deny	Inherited From
Approve	☒	☐	Modules
Archive	☒	☐	Modules
Create	☒	☐	Modules
Delete	☒	☐	Modules
Read	☒	☐	Modules
Write	☒	☐	Modules

URI

Menu Eligible ☐

The table lists the actions for the resource that can be set to Allow or Deny, and if the permissions were inherited.

Note If neither the Allow nor Deny check box is selected, the role inherits permissions from its parent resource.

Action. Approve, Archive, Create, Delete, Read, and Write. Every resource has Read, which allows the role's users to view the data.

Allow. Select to grant access to the action. Allow grants a role's users permission to use all functionality in the designated area.

Deny. Select to implicitly deny access to the action. Deny provides no access and prohibits a role's users from viewing or changing the designated area.

Inherited From. When a particular resource has inherited permissions from a parent, the relationship is indicated in the Inherited From column.

Note In order for a user to be able to approve, archive, create, delete, or write, that user's role must have read access to the resource.

The different resource types have different actions associated with them, as shown in Table 6.1. Browsers, views, and reports have one line in their permissions tables for allowing or denying read access, while business entities have five lines for approve, create, delete, read, and write.

Table 6.1
Resource Permissions

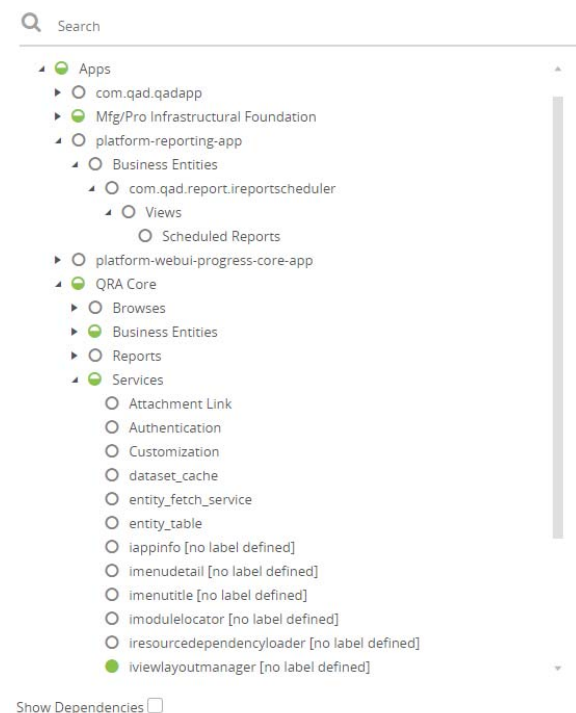
Resource Type	Actions
App	Approve, Create, Delete, Read, Write
Business Entity	Approve, Create, Delete, Read, Write
Browse	Read
View	Read
Report	Read
Service	Create, Delete, Read, Write
Dashboards and KPIs	Delete, Read, Write
Field	Read, Write
Field Group	Read, Write

Below the permissions table is the resource URI and the Menu Eligible check box. This check box identifies those resources that can be added to a role menu. It is for informational purposes and cannot be changed.

Permissions Tree

Resources are arranged in a hierarchy and may have multiple permission types. Figure 6.10 shows the expanded permissions tree for the VP Logistics role.

Fig. 6.10
Role Permissions Tree



A solid green circle represents full access to the actions associated with the resource. A white circle with a gray outline represents no access. A half-green circle indicates partial access. In the tree, the circle next to Apps is half green, which indicates the role has been granted access to some—but not all—resources in the tree. The role has no access to the platform reporting app and partial access to QRA Core. The circle next to platform-reporting-app is white with a gray outline, as is every circle nested below it, indicating no access to any of those resources. The circle next to QRA Core is half green, indicating partial access to the resources that make up QRA Core. The QRA Core branch of the tree contains Services, which also has a half-green circle. Within the Services branch is iviewlayoutmanager, which has a solid green circle, indicating full access to the resource.

Permissions Tree Search

You can search for resources using the Search feature at the top of the permissions hierarchy tree. The search begins at the currently selected level and searches downward. For example, if you select Base App under System|Apps, the search returns matching criteria located in Base App and its child resources. If you want to search the entire system, ensure that System is selected at the top of the tree.

Note The name of the currently selected resource turns blue in the permissions tree and is displayed in the Search field until you start entering text.

By default, the Search field is limited to 48 characters.

Fig. 6.11
Permissions Search

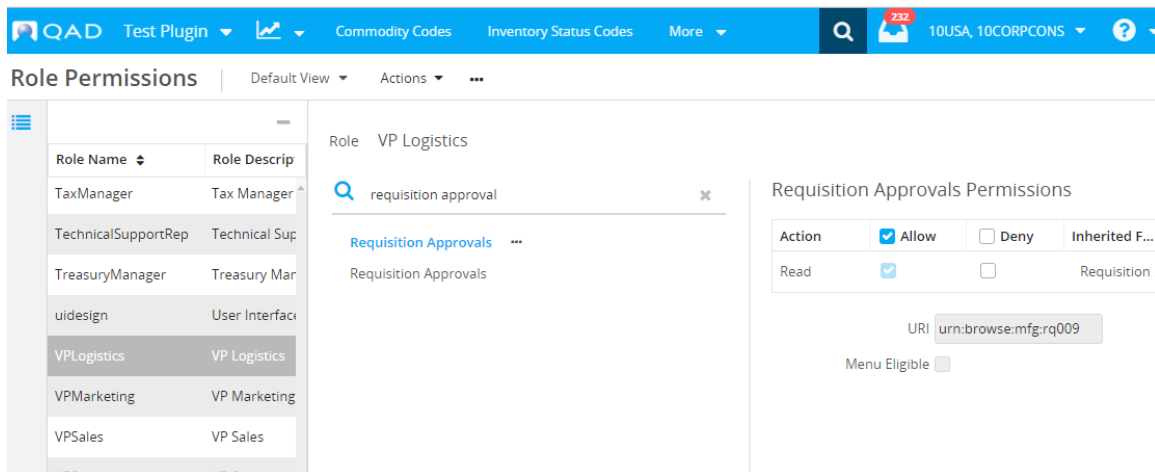
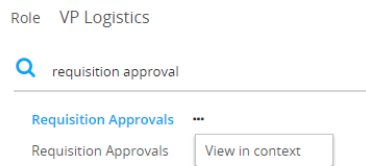


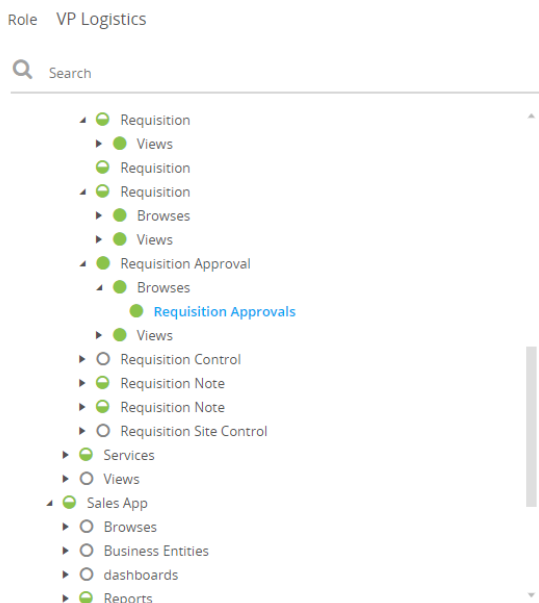
Figure 6.11 shows the search results for requisition approvals for the VP Logistics role. You can click on the search result resources to view and update their permissions. If you need more information to determine which result is the resource for which you were searching, you can view the resources within the context of the permission hierarchy.

Fig. 6.12
View Search Results in Context



- 1 Select one of the resources.
- 2 Select the More icon.
- 3 Select View in context.

Fig. 6.13
Expanded View in Context



- 4 The Permission Tree expands to show where the resource, in blue, fits into the hierarchy, as in Figure 6.13. If you determine this was not the resource for which you were searching, you must start with a new search of the original term.

Resource Dependencies

Resources often depend on other resources to create the different elements of the Channel Islands UI. These dependent entities must be secured independently from the main view. The software automatically identifies dependencies and sets permissions as needed.

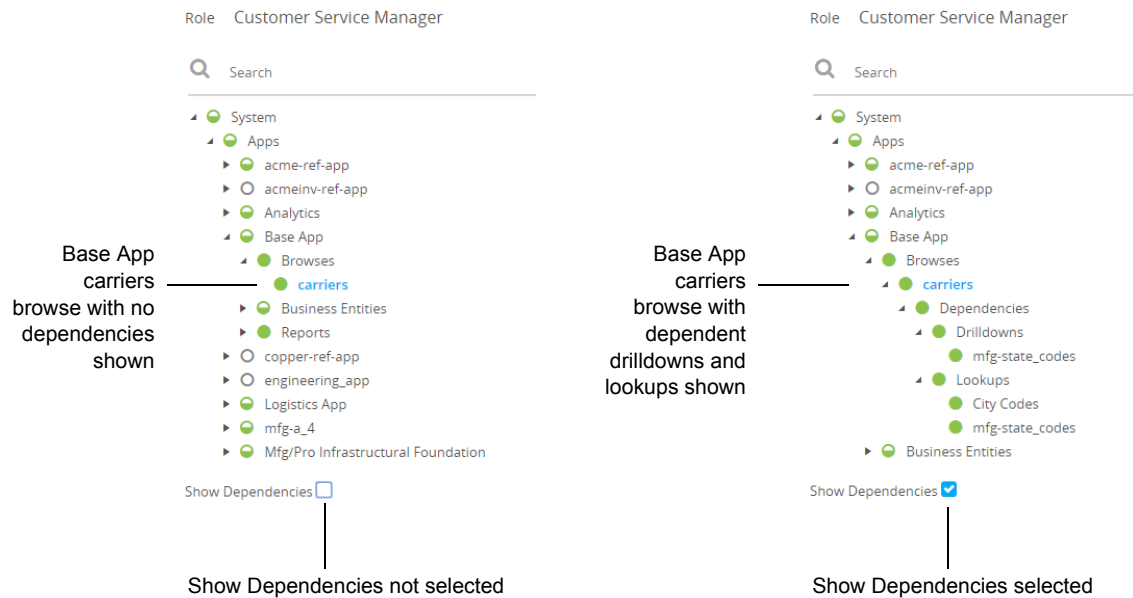
Show Dependencies Check Box

You can view resource dependencies by selecting the Show Dependencies check box on Role Permissions. When the check box is selected, the permissions tree expands to display information on the resource dependencies that exist in the system. Dependencies folders appear in the tree, showing the other resources that are required to populate the main view.

Browses in one business entity can be lookups or drill-downs for a different business entity. For lookups and drill-downs to function correctly, users must have read permission to the associated browse.

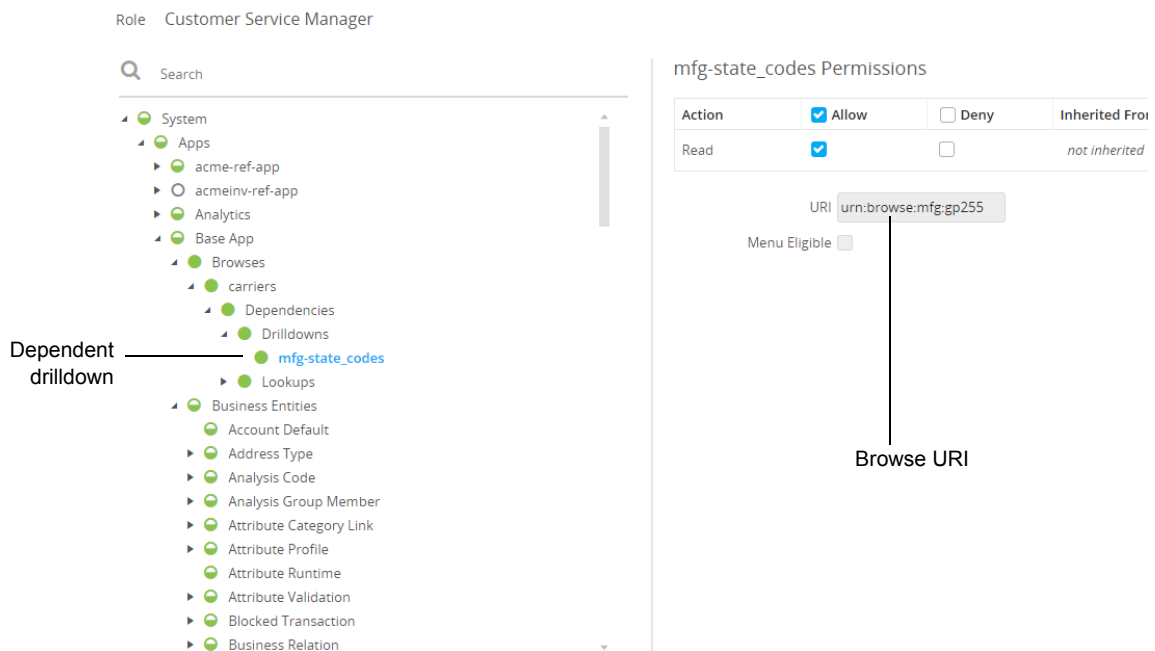
Figure 6.14 shows the Customer Service Manager role in Role Permissions. The example on the left does not have the Show Dependencies box selected. In Base Apps, the only resource within Browses is carriers. However, the example on the right is the same role, this time with Show Dependencies selected. The tree now displays the drill-downs and lookups that must be secured for a role to have full access to the carriers browse.

Fig. 6.14
Show Dependencies



One of the dependencies for the carriers browse in Figure 6.14 is the mfg-state_codes drill-down, shown in Figure 6.15. The URI identifies the mfg-state_codes resource as a browse. In order for the carriers browse to access state codes, the mfg-state_codes browse must have read access.

Fig. 6.15
Browse Example



The software is designed to automatically assign the needed permissions to dependent resources. The Show Dependencies functionality is provided for reference and troubleshooting.

Role Permissions Actions

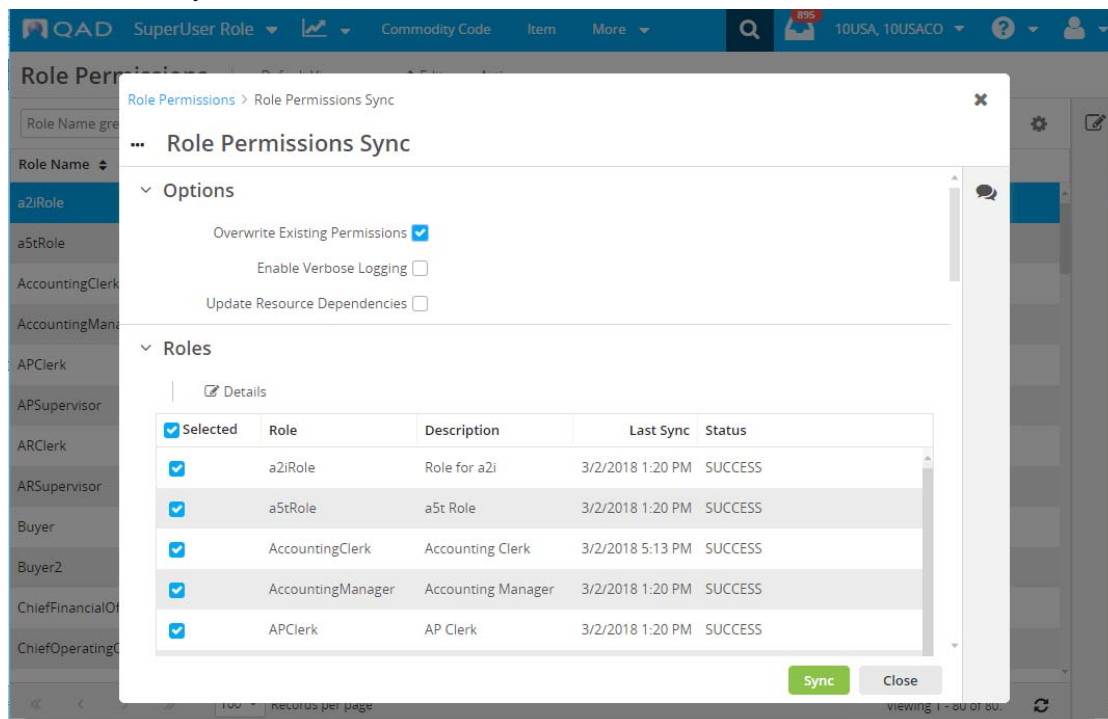
The following actions are available from the Actions menu on the Role Permissions browse, not the hybrid view. If you only see Clear Permissions in the Actions menu, close the hybrid view so you only see the list of system roles.

Role Permissions Sync

Role Permissions Sync synchronizes the settings in the Channel Islands UI based on the settings defined in Enterprise Edition. The action updates permissions that have been configured on the Secured Resources tab of Role Permissions Maintain (36.3.6.5) in the QAD .NET UI. Run this action if you set up or change role permissions using Role Permissions Maintain.

- 1 Select Role Permissions Sync from the Actions menu.
- 2 Select Overwrite Existing Permissions.

Fig. 6.16
Role Permissions Sync



- 3 If you are updating all roles, leave them all selected. If you are updating specific roles, clear the Selected check box and then select only those roles that should be updated.
- 4 Select Sync. The synchronization can take a few minutes to complete.

Update Site Security Using Role Permissions Sync

You must run Role Permissions Sync after you add users to Channel Islands and configure their roles, domains, entities, and sites in User Access. This synchronization updates site security and only needs to include the webui_user role.

- 1 Select Role Permissions Sync.
- 2 Select Overwrite Existing Permissions.
- 3 In Roles, clear the Selected check box.
- 4 Scroll to webui_user and select the role.
- 5 Select Sync. The synchronization can take a few minutes to complete.

Refresh Permissions

Use the Refresh Permissions action if you make updates to role permissions through Role Permissions Maintain in the QAD .NET UI and want the permissions to be updated immediately in the Channel Islands UI. If you do not refresh the permissions using this action, users will not see updated permissions until the cache automatically updates, which could be 24 hours depending on the settings.

Assigning Permissions to Roles

Channel Islands UI securable resources are listed in the Permissions tree on Role Permissions. In order to access and view any of these components in the Channel Islands UI, a role must have the Allow check box selected for the corresponding resources in the Permissions Table.

Note Use role menus to accurately and efficiently set permissions on new roles. See “Role Menu” on page 76 for more information.

Every Channel Islands UI screen corresponds to a view resource that is identified with a resource URI. The view resource is secured based on the business entity associated with the view. The view may require data from other business entities, such as a master screen’s subordinate detail screens, lookups, and services. If a user needs access to a given Channel Islands UI screen, that user’s role needs access to a variety of other resources for the user to have the full functionality of that screen. If the user’s role does not have sufficient permissions for the different resources, the user is presented with an “Error 403: Access Denied, You do not have permission to access the requested page.” For information on identifying dependent resources and missing permissions, see “Role Menu Dependency” on page 93.

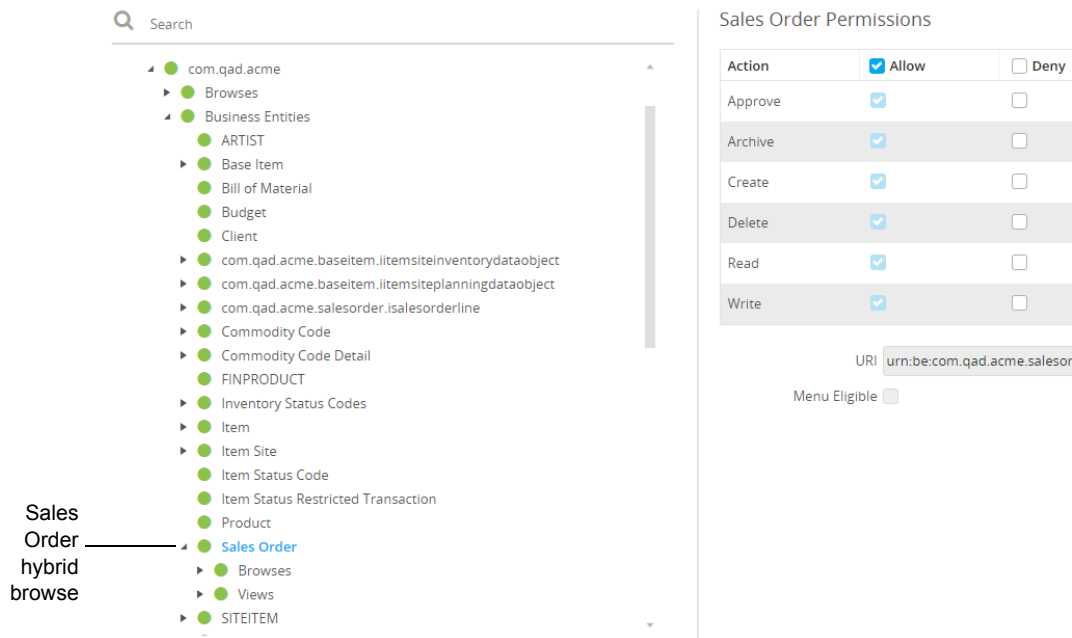
The Channel Islands UI elements are:

- “Hybrid Browse Screens” on page 90
- “Single Row Edit Grids” on page 90
- “Browses” on page 91
- “Lookups and Dashboard Panels” on page 92
- “Fields and Field Groups” on page 92

Hybrid Browse Screens

Hybrid browse screens allow you to view both a static data table and the table's associated, interactive elements, such as a requisition and that requisition's lines. The secured resources for hybrid browses are located in the Business Entities branch of an app's secured resources tree, as illustrated in Figure 6.17. The associated browse resources, view resources, and Field Groups are collected and can be secured from here. Permissions for hybrid browse screens must be set and managed from the business entity level in order to provide, at a minimum, read access to the screen.

Fig. 6.17
Hybrid Browse



Note This level of permissions is only for the master hybrid browse screen entity. Associated lookup tables that have not been linked to the business entity in the `secureresource.xml` file and business entities for related single row edit grids must be configured separately.

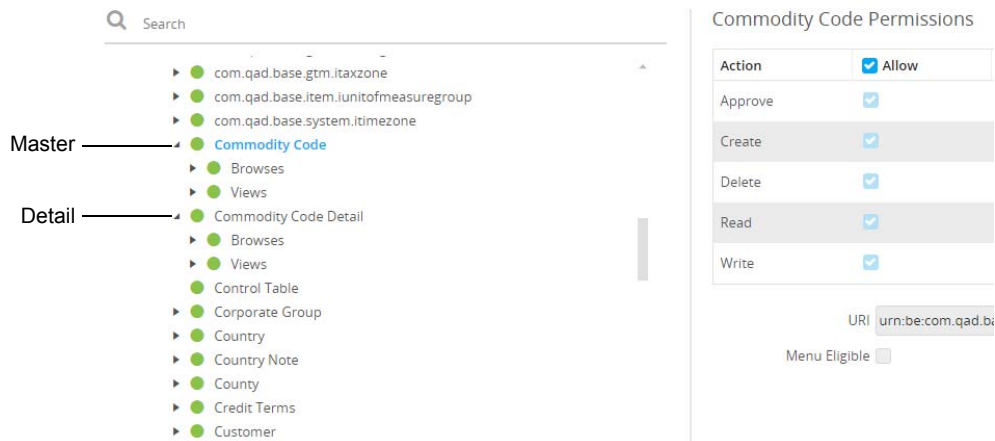
Single Row Edit Grids

Once permissions have been set for hybrid browse screens at the business entity level, some of the screen elements may require additional permissions configuration to ensure complete access to all screen elements on the hybrid browse screen. This includes single row edit grid business entities.

Single row edit grids have their own hybrid browse screens accessible in the grid details window, which means they have their own Business Entity resources that require permission configuration. These resources must be identified and configured in addition to the master entity.

In Figure 6.18, the `ICommodityCodeDetail` business entity is the entity for the Commodity Code Items Grid on the ACME Commodity Code Screen. Permissions must be set for the Master entity and the Details entity to provide complete access to the screen.

Fig. 6.18
Single Row Edit Grid



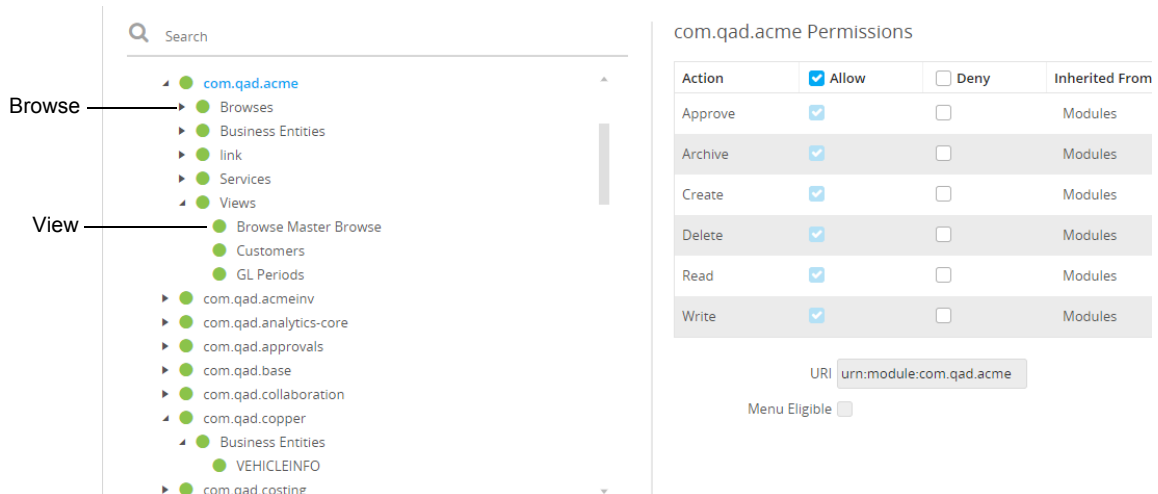
Browses

Browses are the QAD .NET UI, Progress-based “.p” browse programs that serve as power browses or lookup browses. A browse displays data in a read-only table. You cannot edit or delete the existing data, nor add additional records to the browse. You can filter the view.

Before a user can open a browse and view its data, you must assign the correct read permissions to both the associated Browse and View resources. Permission to the Browse resource gives the user access to the data that loads into the screen, and permission to the View resource makes the screen available in the Channel Islands UI menus.

To configure access, you must find the associated browse resource in the Browsers branch of the Permissions tree and the associated view resource in the Views branch of the Permission tree.

Fig. 6.19
Browse Screen



Lookups and Dashboard Panels

Data linked to lookup tables and dashboard panels are also secured resources. In some cases, these resources are used in multiple places across the Channel Islands UI, such as with a Business Entity and a lookup table on a different screen. When configuring permissions for these resources, access may already have been granted from another place. However, if a lookup table is not associated with a Business Entity, you must set its permissions to read access or users receive an access denied message when they attempt to open the lookup table from the screen. When a dashboard panel does not have read access, the system displays “NO_DATA_RETURNED” in the panels.

Note This message does not always indicate that access is not configured for dashboard panels. The message also displays if there is actually no data in the back end.

Note Lookup tables and dashboard panels only require permissions configuration in the associated Browses section of the Secured Resources tab. These screen elements do not have associated view resources.

Fields and Field Groups

Individual fields and groups of fields are resources that can be secured. Fields and field groups only have read and write permissions. If you determine that more fields in your system need to be secured, contact QAD Services.

Note Because Roles and Permissions are set at the system level, field security also must be set at the system level to avoid fields being inaccessible to users in different apps.

The format of a field URI is: `urn:field:com.qad.module.IBusinessEntity:TableName.FieldName`. This string consists of the following sections:

urn:field: •Prefix that identifies this URI as a field.

com.qad.module.IBusinessEntity. •Name of the business entity that owns the field.

TableName. •Name of the table to which this field belongs.

FieldName. •Name of the field.

Fields

Fields can be secured from the Role Permissions screen and can be identified by their URI, which includes the word *field*, as shown in Figure 6.20.

Fig. 6.20
Field

Field

Search

- Name
- Name
- Name
- Name
- Postal Code
- Postal Code
- Primary
- Reported (IN)
- Secondary
- State
- State
- State Tax
- State Tax
- supplier.countrydescription (no label defined)
- supplier.countrydescription (no label defined)
- supplier.deliveryconditioncode (no label defined)
- supplier.disallowedactions (no label defined)
- supplier.disallowedactionsmessage (no label defined)
- supplier.financechargeglprofiledesc (no label defined)
- supplier.ispaybankcharge (no label defined)

State Permissions

Action	☒ Allow	☐ Deny	Inherited From
Read	☒	☐	Modules
Write	☒	☐	Modules

URI: urn:field:com.qad.base.supplier.ISupplier.Supplier.StateCode

Menu Eligible ☐

Required ☐

Field URI

Field Groups

A field group applies permission inheritance to each field within the group. Field groups can be secured from the Role Permissions screen and can be identified by their URI, which includes the words *container:fg*, as shown in Figure 6.21.

Fig. 6.21
Field Groups

Field Group

Search

- icarriercontrol [no label defined]
- idockcontrol [no label defined]
- imfgemployee [no label defined]
- Item
 - Browses
 - Field Groups
 - default
 - Description 1
 - Description 2
 - Design Group
 - Drawing
 - Drawing Loc
 - Drawing Size
 - Item Group
 - Item Revision
 - Item Status
 - Item Type
 - PO Receipt Status

Field Groups Permissions

Action	☒ Allow	☐ Deny	Inherited Fr...
Read	☒	☐	Modules
Write	☒	☐	Modules

URI: container:fg:com.qad.base.item.IItem

Menu Eligible ☐

Field Group container:fg URI

Manually Adding Resources

To add additional secured resources to the Channel Islands UI, contact QAD Services or Support.

Role Menu Dependency

The Role Menu Dependency browse displays every role's resources and resource dependencies. You can use the browse to determine resource dependencies and identify missing permissions for resources in your system.

Fig. 6.22
Role Menu Dependency

RoleName	ResourceURI	Level	DependencyURI	StringCode	Permissions	MenuEligible
VPSales	urn:browse:mfg:cr002	0	urn:browse:mfg:cr002	mfg-SALES_ACTIVITY_DIARY	Read	false
VPSales	urn:browse:mfg:cr003	0	urn:browse:mfg:cr003	PROFILES	Read	true
VPSales	urn:browse:mfg:cr004	0	urn:browse:mfg:cr004	mfg-SALES_FUNNEL_BY_QUARTER	Read	false
VPSales	urn:browse:mfg:cr004	1	urn:browse:mfg:gp163	mfg-ITEM_LOCATION_DETAIL_Q...	Read	false
VPSales	urn:browse:mfg:ic007	0	urn:browse:mfg:ic007	mfg-STOCK_AVAILABILITY	Read	true
VPSales	urn:browse:mfg:ic007	1	urn:browse:mfg:gp072	Code Master	Read	false
VPSales	urn:browse:mfg:ic007	1	urn:browse:mfg:gp197	Item Descriptions	Read	false
VPSales	urn:browse:mfg:ic007	1	urn:browse:mfg:gp340	Item Master	Read	false

RoleName. The name of the role.

ResourceURI. The URI associated with each label item.

Level. The level of the resource within the permission tree. Either 0 or 1. A level 0 is dependent on itself. Level 1 resources are dependent on the associated ResourceURI.

DependencyURI. The URI of the dependent resource. If the level for the ResourceURI is 0, this value is the same as ResourceURI.

StringCode. The translatable value associated with this ResourceURI.

Permissions. The permissions that are currently set for the associated resource. If this column is blank, the resource has not been secured. Use this column to determine which resources are missing permissions and need to be secured.

MenuEligible. Does this resource appear as a selectable item on a menu. True or false.

Use the search options to narrow your results. If a user has been denied access to a screen, ensure that you have the user's role before beginning your search.

Using the Information on Role Menu Dependency

- 1 Identify which resources have not been properly secured and are missing permissions. In particular, look for resources in the Permissions column that do not have adequate permissions.
- 2 Copy the URI of the resource requiring permission.

Note Because the Search field on Role Permissions has, by default, a 48-character limit, copy the end of the URI to ensure your search returns the most relevant resources. If you try to paste more than 48 characters, only the first 48 will appear in the field and be searched.

- 3 Go to Role Permissions.
- 4 Edit the role that requires access to the denied resource.

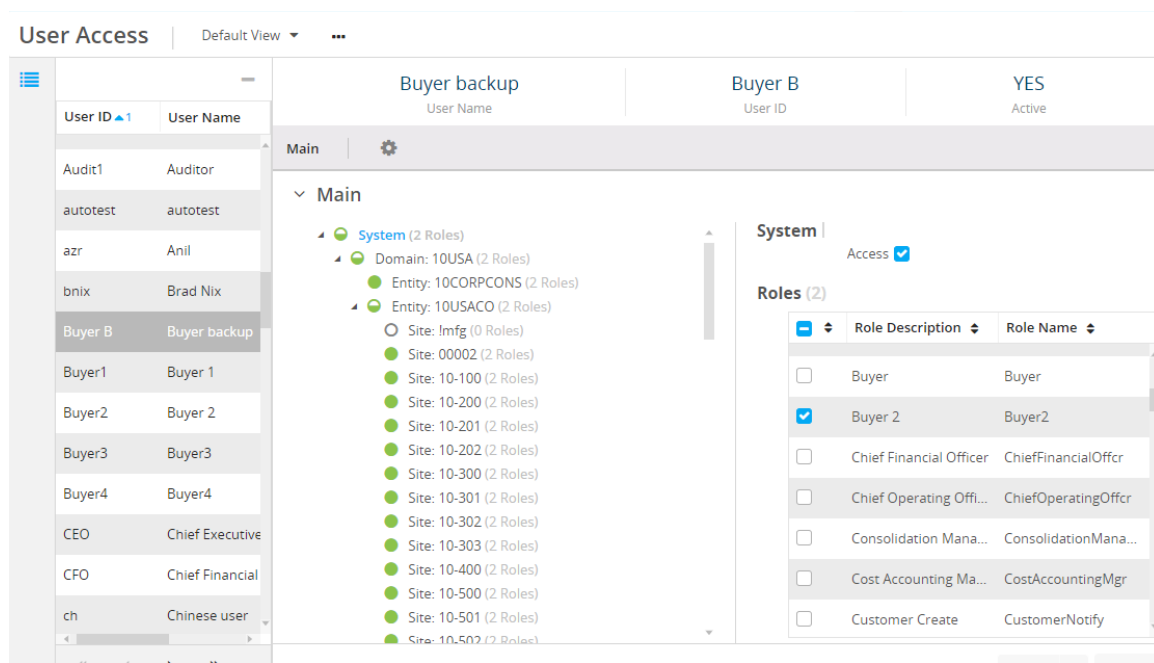
- 5 In the Search field, paste the URI of the resource requiring permission.
- 6 Select the resource.
- 7 Grant the necessary permission in the permission tree and save.

User Access

Every Channel Islands UI user must be assigned at least two roles, one of which is webui_user. A user cannot access the Channel Islands UI without the webui_user role, but can still access the QAD .NET UI. User Access allows administrators to configure user access to domains, entities, and sites, and to assign users to roles within the areas of QAD to which they have access.

Note Modifying site security on the User Access screen does not change site security settings in the QAD .NET UI nor on Site Security in the Channel Islands UI.

Fig. 6.23
User Access



Set System Access

The System tree is a hierarchical view of all domains, entities, and sites within Channel Islands. To the left of each item is a circular status indicator that displays the status of the Access check box in the right-hand panel, located above the Roles list. A solid green circle indicates that the Access check box is selected and the user has access to that area of Channel Islands and to all items lower in the tree. A white circle with a gray border indicates that the user has no access to the associated item, nor to items lower in the tree. A half-green circle indicates that the user has access to some but not all of the areas of Channel Islands lower in the tree.

Sites are the lowest level of the hierarchy and can only be a solid green circle, meaning full access, or a solid white circle with a gray border, meaning no access. System, domains, and entities can be all green, all white, or half-green circles because their child elements can be a mix of access and no access.

Access is assigned in a top-down manner, with automatic inheritance for child items. When you grant access to a parent element, all children of that element are granted access. You can remove the access for items lower in the tree by clearing the Access check box for those child items one by one. If you clear the Access check box of a parent element, no children of that element can have access. You cannot select the Access check box of a child element when a parent element has the Access check box cleared.

In Figure 6.23, the user has access to Entity 10CORPCONS and to all sites in 10USACO except the first one, !mfg. Because the user does not have access to the !mfg site, the circle next to the site's parents, Entity 10USACO, Domain 10USA, and the System, are half green, indicating the user has access to some but not all of the system's elements.

Fig. 6.24
Roles Grid

10CORPCONS | USA CORP. CONSOLIDATION

Access ☒ Default Entity ☐

Active Entity ☒

Roles (2)

☒	Role Description	Role Name
☐	AP Supervisor	APSupervisor
☐	AR Clerk	ARClerk
☐	AR Supervisor	ARSupervisor
☐	Buyer	Buyer
☒	Buyer 2	Buyer2
☐	Chief Financial Officer	ChiefFinancialOffcr
☐	Chief Operating Officer	ChiefOperatingOffcr
☐	Consolidation Manager	ConsolidationManager
☐	Cost Accounting Mana...	CostAccountingMgr
☐	Customer Create	CustomerNotify

Assign Roles

The Roles grid displays all of the roles in the area of QAD selected in the user access tree and listed at the top of the grid. The Access check box controls whether a user has access to the associated area of Channel Islands. You can only edit the Roles grid when the Access check box is selected.

Figure 6.24 shows the roles in entity 10CORPCONS. You can modify role assignments for the selected user using the Roles grid. Select or clear the check boxes next to roles to grant or deny access to the selected area of the Channel Islands UI.

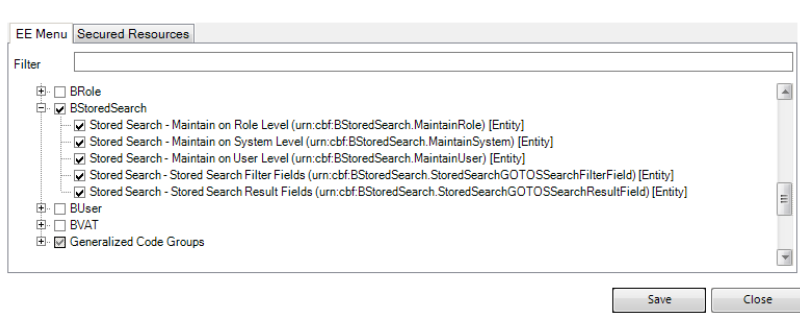
Configure Stored Views Access

You can create and use stored views in the Channel Islands UI that customize screen layout, emphasizing important information needed for everyday use and specific tasks. Depending on the role, you may need to configure different levels of access for the types of stored views a user can create, edit, or delete.

Stored-view security must be configured for each role and is completed in Role Permissions Maintain in the .NET UI. To enable this feature, double-click a role, then set permissions on the EE Menu tab. Under Secured items not on menu, expand BStoredSearch.

Note The Stored Search check boxes do not secure or affect stored searches in the Channel Islands UI.

Fig. 6.25
Stored Views



Depending on the access required for this feature, you can grant access to any of the following options, then click Save:

- **Stored Search – Maintain on User Level.** Allows users to create personal views that only they can view and manage. It is recommended that all users have the ability to customize their own views.
- **Stored Search – Maintain on System Level.** Allows users to create and manage System views that every user who has access to the Channel Islands UI can view.
- **Stored Search – Maintain on Role Level.** Allows users to create and manage role views that every user assigned to that role can view.

To ensure that all users can configure and save individual views, select Stored Search – Maintain on User Level for the webui_user role. It is recommended that you grant access to the Role Level and System Level options for the QAD Admin role, the SuperUser role, and any other admin roles in your system.

QAD .NET UI Security

This section discusses how to set up additional types of security for your system.

SSH on the QAD .NET UI 100

Describes the settings for SSH.

Public Key Authentication for SSH 101

Explains how to set up public key authentication.

SSH for QAD .NET UI Terminal Mode 103

Explains the safeguards of using SSH instead of telnet.

SSL on QAD .NET UI Tomcat Home Server 103

Describes how to set up SSL on the QAD .NET UI Tomcat Home Server.

HTTPS for QAD .NET UI Desktop Screen Display 106

Explains how to set up HTTPS for QAD .NET UI Desktop screen display.

HTTPS for AIA 107

Describes how to set up AppServer Internet Adapter (AIA) with HTTPS.

Additional Security for Standard Programs 107

Describes how to use the system to add security functions and limitations to specific user IDs and roles, control inventory updates, and define general ledger account security.

SSH on the QAD .NET UI

As of QAD NET UI 2013 EE (3.0.0), the Connection Manager specifies secure shell (SSH) rather than telnet by default.

To view and change the settings, in Administration | Connection Manager, under Functions, click Update configuration settings:

Host. The machine name or IP address of the SSH or telnet server.

Port. The port number for SSH or telnet. The default is 22 (SSH). For telnet, the port number is 23. (Previously, the default was 23 for telnet).

Protocol. Specifies the connection protocol as ssh (the default) or telnet. (Previously, the default was telnet.)

Startup Script. The server sign-in prompts and the responses to these prompts, separated with the pipe symbol (|). The standard order is:

```
loginPrompt|userid|passwordPrompt|$PASSWD|osPrompt|cd
UIConfigDir|osPrompt|startScript
```

For example:

```
login:|mfg|Password:|$PASSWD|$|cd /user/mfg/work|$|exec
/user/mfg/work/scripts/connmgr.wrap
```

Note The same startup script can be used for both SSH and telnet. If using SSH, the sign-in credentials in the script are ignored if they are specified in the Server Startup User and Server Startup Password settings. For SSH, if you have defined Server Startup User and Server Startup Password, you can remove the sign-in credentials from the script, but the first four token delimiters still must be included in the script. For example, for telnet, the script might be:

```
login:|mfg|Password:|$PASSWD|$|cd /user/mfg/work|$|exec
/user/mfg/work/scripts/connmgr.wrap
```

For SSH, however, with the sign-in credentials defined in Server Startup User and Server Startup Password, the script can be:

```
|||||$|cd /user/mfg/work|$|exec /user/mfg/work/scripts/
connmgr.wrap
```

Server Startup User. Specifies the user ID of the server startup user, if not specified in the startup script. This setting is only used for SSH.

Server Startup Password. The password for the session startup script, if not specified in the startup script. It is encrypted on entry.

SSH Private Key File. If using public key authentication, described on page 101, enter the directory path to the private key file. For example, /directory/path/id_rsa.

SSH Private Key Password. If using public key authentication, described on page 101, enter the passphrase.

Public Key Authentication for SSH

SSH supports both password-based authentication and public key authentication. By default, the QAD .NET UI uses password-based authentication, but you can set up public key authentication instead.

Public key authentication is an authentication method that relies on a generated public/private keypair. The keypair is generated using public key cryptography that has the mathematical property that prohibits the same key from encrypting and decrypting the same message. The keys are used at the protocol level for authentication inside SSH during session creation.

It is important to protect the privacy of the private key file. The private key file can be encrypted with a password to ensure that even if someone were to obtain the private key file it would be useless. The SSH public key authentication implementation supports both password protected and unencrypted private key files.

To set up public key authentication:

- 1 Sign in to the server as the user specified in the Connection Manager settings for Startup Script or Server Startup User. After signing in, go to your .ssh directory:

```
$ cd $HOME/.ssh
```

- 2 Generate your public/private RSA keys with a blank passphrase:

```
$ ssh-keygen -t rsa
```

```
Generating public/private rsa key pair.
```

```
Enter file in which to save the key (~/.ssh/id_rsa): (press return)
```

```
Enter passphrase (empty for no passphrase): (press return)
```

```
Enter same passphrase again: (press return)
```

```
Your identification has been saved in ~/.ssh/id_rsa
```

```
Your public key has been saved in ~/.ssh/id_rsa.pub
```

```
The key fingerprint is:
```

- 3 Ensure that your .ssh directory has the correct permissions:

```
$ chmod 700 .ssh
```

- 4 Copy the contents of your public key “id_rsa.pub” into your .ssh/authorized_keys file:

```
$ cat id_rsa.pub >> authorized_keys
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAABJQAAAIEAlW5CbYdQXy4hmLVZq2A8uMKk6eZyNF+r6a  
k23RUHyxscAm7EEysD4lnDW1sbdc1aEEKPowcXKYOG4h1RkJbjz8KBj6kYeplo  
60NEg6Vm+q+MUzdm99CdneN0fQHEjvTxyBCvyUx+dotK0l0DuCteMHsASuyTW  
q37X0bHyEcBxE= rsa-key-20130418
```

- 5 Ensure that your public/private keys have the correct file permissions:

```
$ chmod 600 id_rsa.pub
```

```
$ chmod 600 authorized_keys
```

The private key file needs to be accessible by the user that started Tomcat. Put it in a location accessible by that user and change its owner and permissions:

```
$ chown <tomcat user>:<tomcat group> id_rsa
$ mv id_rsa tomcat/webapps/<app name>/WEB-INF
$ chmod 600 tomcat/webapps/<app name>/WEB-INF/id_rsa
```

Add a Passphrase to Private Key File

Use the following command to add or change a passphrase to an existing private key file.

- 1 If not already in your .ssh directory, go to your .ssh directory:
\$ cd .ssh
- 2 Add a passphrase to your private key stored in the id_rsa file:
\$ ssh-keygen -f id_rsa -p
Key has comment 'id_rsa'
Enter new passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved with the new passphrase.

Connection Manager Configuration Screen Settings

Finally, in the Connection Manager configuration screen, set the following:

In *Startup Script*, remove the sign-in and password entries but leave all the other text including the pipe symbols (|).

For example, if the setting for *Startup Script* is:

```
login:|qad|Password:|qadpass|$|cd /home/demo|$|/dr01/qadapps/qdt/
envs/live/scripts/connmgr.live
```

Change it to:

```
login:||Password:|||$|cd /home/demo|$|/dr01/qadapps/qdt/envs/live/
scripts/connmgr.live
```

In *Server Startup User*, enter the user ID.

In *Server Startup Password*, remove any value. This field should be blank.

In *SSH Private Key File*, enter the directory path to the file (for instance, /directory/path/id_rsa).

In *SSH Private Key Password*, enter the passphrase.

Troubleshooting Tips

If the Connection Manager sessions are not connecting properly via SSH and are stuck in the initializing state, check the following:

- Check the desktop.log file (tomcat/webapps/<app_name>/WEB-INF/logs) for connection errors.
- On Linux, check the /var/log/secure file for SSH connection errors.
- Some systems using SSH require that the home directory of the SSH user be owned by the SSH user. For example, if the user is telnet and the home directory is /home/telnet, then make sure that the owner of that directory is telnet and that it belongs to the same group as telnet.
- Some systems using SSH require that the home directory of the SSH user have certain permissions. Set the permissions to 700; for example, `chmod 700 /home/telnet`.

SSH for QAD .NET UI Terminal Mode

For QAD .NET UI terminal mode display, you can use SSH (Secure Shell) rather than standard telnet. SSH is a protocol that can create a secure connection between a QAD .NET UI client and the server.

The safeguards that SSH provides include:

- User authentication and key exchange
- Negotiated encryption, compression, and message integrity verification
- All data encrypted using a symmetric key algorithm and verified against a keyed-hash message authentication code (HMAC)

The steps to set up SSH for QAD .NET UI terminal mode are included in the “SSH and Telnet Protocols” appendix of the *QAD Enterprise Edition Installation Guide*.

SSL on QAD .NET UI Tomcat Home Server

The following steps describe how to set up SSL on the QAD .NET UI Tomcat Home Server. Be sure to review the Apache Tomcat documentation on this topic. For example, see:

http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html#SSL_and_Tomcat

- 1 Create a keystore file to store the server’s private key and SSL certificate. Make sure that \$JAVA_HOME/bin is in your PATH. The following example uses Java 1.6.

```
$ cd $TOMCAT_HOME/bin
$ mv keystore keystore.bak # save the old keystore
$ keytool -genkey -alias tomcat -keyalg RSA -dname "CN=
vmnnn01.qad.com,OU=QAD,O=QAD,L=Santa Barbara,ST=California,C=
US" -keystore keystore -keysize 2048 -storepass changeit -
keypass changeit
```

Note The Common Name (CN) is the name of the web server as it will be referenced from a browser. For example, CN=vmnnn01.qad.com.

View keystore

```
$ keytool -list -v -keystore keystore -storepass changeit
```

The response is as follows:

```
Your keystore contains 1 entry
Alias name: tomcat
Creation date: Oct 18, 2011
```

```

Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=vmnnn01.qad.com, OU=QAD, O=QAD, L=Santa Barbara, ST=California, C=US
Issuer: CN=vmnnn01.qad.com, OU=QAD, O=QAD, L=Santa Barbara, ST=California, C=US
Serial number: 4e9dbf82
Valid from: Tue Oct 18 11:03:46 PDT 2011 until: Mon Jan 16 10:03:46 PST 2012
Certificate fingerprints:
  MD5: FE:B4:69:FA:78:CA:D1:3E:41:5D:A8:1C:6A:F3:E4:CF
  SHA1: FD:DF:94:3A:A8:74:76:C3:4F:AC:8A:60:9A:94:5A:C0:8C:9A:11:3E
Signature algorithm name: SHA1withRSA
Version: 3

```

For this example, the default password of `changeit` is being used.

Make sure you back up your keystore because it contains your public/private keys.

- 2 Generate a Certificate Signing Request (CSR) required by the certificate provider into the file `certreq.csr`.

```
$ keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr
-keystore keystore -storepass changeit
```

- 3 You will receive an SSL certificate and a Primary Intermediate CA certificate file. You need to install the Primary Intermediate CA certificate first. GeoTrust issues these files in PKCS#7 format. Open a file named `primary.p7b` in the vi editor and copy the Primary Intermediate CA certificate into the file. The contents look like this:

```
-----BEGIN CERTIFICATE-----
```

```

MIID2TCCAsGgAwIBAgIDAjbQMA0GCSqGSIb3DQEBBQUAMEIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1HZW9Ucn
VzdCBjbmMuMRswGQYDVQDEJHJW9UcnVzdCBHbG9iYWwgQ0EwHhcNMTAwMjE5OTI2WhcNMjAwMjE5OTI2WjBAMQsw
CQYDVQGEwJVUzEXMBUGA1UEChM0R2VvVHJ1c3QsIEluYy4xGDAWBgNVBAMTD0dlb1RydXN0IF
NTTCBDDQTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJCzgmHk5UatcGA9uuUU3Z6KXot1WubKbUGl
I+g5hSZ6p1V3mkihkn46HhrxJ6uJTDnMyz1Hr4GuFmpcN+9FQf37mpc8oE0dxt8XIdGKolbCA0mEEoE+yQpUYG
a5jFTk+eb5lPHgX3UR8im55IaisYmtph6DKW0y8FQchQt65+EuDa+kvc3nsVrXjAVaDktzKITt1XTTYdwvhGLi
cTbi2lYKBeuXy0pU1wozekd0VSQdl+8a5BLGDzAYtDRN4dggj0yFbLTAZJQ5096QhS6CkIMlszZhWwPKoXz4mda
AN+DaIiixafWcwqQ/RmXAueOFRJq9Veis+jDkNd53eAsMMvR8CAwEAAaOB2TCB1jA0BgNVHQ8BAf8EBAMCAQYw
HQYDVR00BBYEFJ5VBthzVurPmPVPEhX9Z/7Rc5KMB8GA1UdIwQYMBaAFMB6mGiNiFurBWQMEX2qfWw4ysxOMB
IGA1UEEwEB/wQIMAYBAf8CAQAwOgYDVR0fBDMwMTAvoC2gK4YpaHR0cDovL2Nybc5nZW90cnVzdC5jb20vY3Js
cy9ndGdsb2JhbC5jcmmwNAYIKwYBBQUHAQEEDAMMCGCCsGAQUFBzABhhodHRwOi8vb2Nzc5nZW90cnVzdC
5jb20wDQYJKoZIhvcNAQEFBQADggEBANTvU4ToGr2hiwTaqVf0RB4RV2yV2p0JMtltjGxKzrUJpjiJ2ZwMZZB
YlQG55cd0prApCLICq8kx6jEmLTBFEx4TctoLF0XpLR4TEbigMMf0HES0tdT41SFULGcy+5j0vhWiu1Vuy7AyB
h3hjELC3DwfjWdpCOTZFznNF0WX30sewYk2k9QbSqr0E1TQcK0u3EDSSmGGM8hQkx0YlEVxw+o78Qn5Rsz3VqI
138S0adhJR/V4NwdzxoQ2KDLX4z6D0W/cf/LXUQdpj6HR/oaTo0DEj+IZpWYeZqF6wJHJzSxj8gYETpnKXKBuer
vdo5AaRTPvvz7SBMS24CqFZUE+ENQ=

```

```
-----END CERTIFICATE-----
```

Then copy the SSL certificate into the file `ssl_cert.p7b`.

- 4 Import the Primary Intermediate certificate (`primary.p7b`) into the Java keystore:

```
$ keytool -import -alias primary -trustcacerts -file
primary.p7b
-keystore keystore -storepass changeit
```

- 5 Import the SSL certificate into the Java keystore (`ssl_cert.p7b`):

```
$ keytool -import -alias tomcat -trustcacerts -file
ssl_cert.p7b -keystore keystore -storepass changeit
```

- 6 Validate the keystore entries:

```
$ keytool -list -v -keystore keystore -storepass changeit | more
```

The response is as follows:

```
Alias name: primary
```

```

Creation date: Oct 18, 2011
Entry type: trustedCertEntry
Owner: CN=GeoTrust SSL CA, O="GeoTrust, Inc.", C=US
Issuer: CN=GeoTrust Global CA, O=GeoTrust Inc., C=US
Serial number: 236d0
Valid from: Fri Feb 19 14:39:26 PST 2010 until: Tue Feb 18 14:39:26 PST 2020
Certificate fingerprints:
MD5: DF:F1:B7:6B:25:8D:BE:73:48:E3:76:68:97:A9:38:71
SHA1: 78:0A:06:F6:E9:B4:06:1C:AD:0C:65:02:71:06:06:EB:53:5F:1C:26
Signature algorithm name: SHA1withRSA
Version: 3
...
Alias name: tomcat
Creation date: Oct 18, 2011
Entry type: PrivateKeyEntry
Certificate chain length: 3
Certificate[1]:
Owner: CN=vmnnn01.qad.com, OU=QAD, O=QAD Inc, L=Santa Barbara, ST=California, C=US,
SERIALNUMBER=haR57ua0G5cC3ZMg5ugxN9t6rjDKEVF/
Issuer: CN=GeoTrust SSL CA, O="GeoTrust, Inc.", C=US
Serial number: f310
Valid from: Sun Oct 16 23:55:13 PDT 2011 until: Thu Oct 18 22:33:33 PDT 2012
Certificate fingerprints:
MD5: E8:76:F2:97:C0:CE:00:0A:AB:01:71:9F:70:21:9E:7F
SHA1: 1D:66:21:6E:C2:E3:58:F2:B5:D2:80:38:C7:E3:5F:FA:BF:7E:89:4B
Signature algorithm name: SHA1withRSA
Version: 3

```

- 7 Uncomment the SSL HTTP/1.1 Connector entry in the \$TOMCAT_HOME/conf/server.xml file. You may have to add the keystorePass attribute and set the value to the keystore password:

```

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="bin/keystore"
keystorePass="changeit"
URIEncoding="UTF-8"
compression="on"
compressableMimeType="text/html,text/xml,application/
xml,application/octet-stream"
/>

```

- 8 Restart Tomcat:

```
$ cd $TOMCAT_HOME/bin
$ ./startup.sh
```
- 9 Port 8443 should be in the LISTEN state.
- 10 Validate the connection by going to the Tomcat home page. For example, go to the following URL:

```
https://vmnnn01.qad.com:8443
```

- 11 Update client-session.xml (HOMESERVER/configurations/<config name>/client-session.xml) to use HTTPS when connecting to Desktop:

```

<!-- The desktop protocol. Valid values are "http" or "https".
-->
<DesktopProtocol>https</DesktopProtocol>
<!-- The Tomcat host name. -->
<DesktopHost>vmnnn01.qad.com</DesktopHost>
<!-- The Tomcat port number. -->

```

```
<DesktopPort>8443</DesktopPort>
```

- 12 Start the QAD .NET UI and open Sales Order Maintenance. You can check the configuration by looking in Help | View Configuration and searching for the `desktopbaseurl` setting. It should look like `https://host:port/qadu.i`.

HTTPS for QAD .NET UI Desktop Screen Display

In the QAD .NET UI, screens that display in Desktop mode are based on XML representations of Character UI screens. By default, the XML is posted to Tomcat with an HTTP request to the `XMLReceiverServlet` for use by the QAD .NET UI. However, instead of using HTTP, you can use HTTPS.

To set up HTTPS for QAD .NET UI Desktop screen display:

- 1 Enable the SSL Connector in Tomcat. See page 103.
- 2 To install the certificate file into Progress you need the certificate in the .pem or .cer format.
- 3 If you do not have this format then use Internet Explorer to export the certificate in the .cer format: Select Internet Options > Content > Certificates > Trusted Root Certification Authorities and then select your certificate. Select Export. Use Base-64 encoded X.509(.CER).
- 4 Take the certificate file and run the following Progress command.
If the certificate is in the .pem format, run:

```
$DLC/bin/mkhashfile <your certificate>.pem
```

 If the certificate is in the .cer format, run:

```
$DLC/bin/mkhashfile <your certificate>.cer
```
- 5 Edit `tomcat/webapps/<appname>/WEB-INF/conf/connectionManagerConfig.xml`. Go all the way to the bottom of the file then go up a few lines to the following element: `<connectionSetupParameter>`. Edit the “value” attribute to use “https” and use the secure Tomcat port.
- 6 Edit `tomcat/conf/server.xml` and find the `<Host>` element near the bottom. Add the following inside that `<Host>` element. This will provide logging to verify that the `XMLReceiverServlet` calls are coming through the https port.

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
      directory="logs"
      prefix="requests_log."
      suffix=".log"
      pattern="port=%p urlpath=%U" />
```
- 7 Restart Tomcat.
- 8 To verify the HTTPS activity, look in the `tomcat/logs` directory for a log file that starts with `requests_log` and tail -f that log file. You should see requests going to the `XMLReceiverServlet` on the https port.

- 9 Once you have done the verification, edit `tomcat/conf/server.xml` and remove the Valve entry that you added in step 6. It was only for verification.
- 10 Restart Tomcat.

HTTPS for AIA

Progress AIA provides Internet access for clients to access an AppServer or Sonic Adapter application. It supports both HTTP and HTTPS. This section describes how to set up AppServer Internet Adapter (AIA) with HTTPS. The following steps assume you have installed AIA and now want to configure it to support HTTPS.

- 1 In the `ubroker.properties` file, update the `httpsEnabled` parameter in the `Aia` section. 0 is disabled and 1 is enabled:
`httpsEnabled=1`
- 2 Update the `client-session.xml` file to use HTTPS with AppServer connections. For example:

```
<!-- MFG AppServer connection -->
<ConnectionProtocol>https</ConnectionProtocol>
<ConnectionHost>vmnnn01.qad.com</ConnectionHost>
<ConnectionPort>8443</ConnectionPort>
<ConnectionService>aia/Aia?AppService=
QADMFG_AS</ConnectionService>
```
- 3 Update `client-session.xml` to secure the MFG Login AppServer connection. For example:

```
<!-- MFG login AppServer connection -->
<ConnectionSecureProtocol>https</ConnectionSecureProtocol>
<ConnectionSecureHost>vmnnn01.qad.com</ConnectionSecureHost>
<ConnectionSecurePort>8443</ConnectionSecurePort>
<ConnectionSecureService>aia/Aia?AppService=
QADMFG_AS</ConnectionSecureService>
```
- 4 Update `client-session.xml` to secure the Financials AppServer URL connection. For example:

```
<!-- Financials AppServer URL -->
<qad.appserver url=
"https://vmnnn01.qad.com:8443/aia/Aia?AppServer=QADFin_AS">
</qad.appserver>
```
- 5 Restart Tomcat.

Additional Security for Standard Programs

In addition to the standard role-based permissions, a number of other types of security can be defined for standard programs. These types of security apply in operational areas.

Using the system, you can:

- Specify user IDs that can update the value of specific program fields.
- Determine which users or roles can create operational transactions that affect:
 - Sites, locations, inventory statuses, and other inventory-related attributes
 - General ledger accounts
 - Inventory movement codes

Note the following fundamental difference in the way role-based security works and the way these additional forms of operational security work:

- For role-based access to domains and entities or resources secured through Role Permissions Maintain, no one has access unless it is specifically granted.
- For other types of operational security, all users and roles have access unless specific access records have been defined. Once access records have been defined, other users and roles are automatically prevented from having access.

If you use the Sales and Use Tax Interface (SUTI) to communicate tax data between the system and Vertex's Quantum for Sales and Use Tax product, set up similar access controls in Tax Interface Control (36.5.3.24). See *Technical Reference: Sales and Use Tax Interface* for information on SUTI.

Access records apply only to the current domain from which they are entered.

Specifying User IDs and Roles

To define security access by field, site, and so on for standard programs, you can enter any number of valid user IDs and/or roles, separated by commas, in the following programs:

- Specify user IDs in Field Security Maintenance (36.3.15.1). See page 109.
- Specify user IDs or roles in Site Security Maintenance (36.3.13.8). See page 112.
- Specify user IDs or roles in GL Account Security Maintenance (36.3.13.1). See page 123.
- Specify user IDs or roles in Inventory Movement Code Security (36.3.13.13). See page 124.

Note If you do not set up records in these programs, the system by default allows access to all users who pass sign-in, domain, and role-based access security restrictions. See “Sign-in Security” on page 17.

The system validates entries against records set up in User Maintenance and Role Create.

The asterisk (*) and exclamation point (!) are special characters when used in the User IDs/Roles field.

- The asterisk (*) gives access to all users and roles.
- The exclamation point restricts specific users by user ID, not by role. For example, !user1, * means all users except user1 have access to the function; !user1, admin allows access only to members of the admin role, with the exception of user1. However, !admin, * does not prevent members of the admin role 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 also must 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, roles, 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 roles. The asterisk allows access to all users assigned the role, even if they have been excluded as individuals.

Table 1.6 lists some examples. User IDs and role names are not case-sensitive.

Table 7.1
Sample Uses of User ID and Role Name

String	Description
<code>*</code>	All users have access.
<code>mary, manager</code>	Only user <code>mary</code> and members of the <code>manager</code> role have access.
<code>!jcd, *</code>	Everyone but user <code>jcd</code> 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.

Limiting Access to Fields

Field security prevents unauthorized users from updating secured fields in standard programs. Field security does not prevent users from seeing the value of a field if they have access to the screen where it is updated. Nor does it protect a field from program-level updates through custom code.

Note Standard field security is not exactly the same as component-based field security. In component-based functions, you can disable and hide fields.

The system determines whether a user is authorized based on whether the user ID matches the values specified for the field.

Enterprise Edition Field Security

The following sections describe field security specific to Enterprise Edition. See “Fields and Field Groups” on page 92 for details on securing fields in the Channel Islands UI.

Field Security Validation

When you install your QAD application, security is not active for any fields, and only a few fields are eligible for field security.

Use the Dictionary Field Security Report (36.3.15.4) to determine which fields can be given security.

In the character interface, you also can 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 that references `gppswd.v`. The syntax is:

```
{gppswd.v &field=<dictionary field name>}
```

Activated Field Security Report

Use the Activated Field Security Report (36.3.15.3) to see which fields have security activated. It also lists privileged user IDs.

Dictionary Field Security Report

The Dictionary Field Security Report (36.3.15.4) 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 roles. 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 (36.3.15.1).
- 2 Verify that the field is secured by running the Activated Field Security Report (36.3.15.3).

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 (36.3.15.1).

For multiple databases, make your security changes in the database against which you compile. The changes are then in effect for any other databases against which you run the compiled code.

- 1 Identify and list all fields to which you want to add security.
Since recompiles take time, it is more efficient to add all field security at once.
- 2 Make sure all other users are signed 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 Next, you are prompted for the next entry.
- 5 Press End to exit Field Eligibility Maintenance.

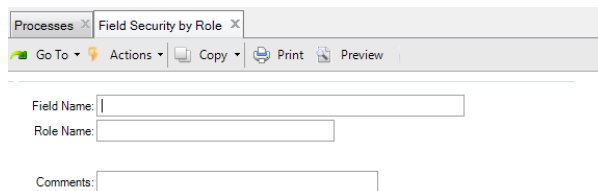
- 6 Recompile either all programs or those programs impacted by the changed field security. If you have custom programs that access these fields, they also need to be recompiled.
To compile only the affected programs, make a backup copy of `utcompil.wrk` in the `qad` directory, and then delete the program 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.
- 9 Verify that each field is secured by running the Activated Field Security Report.

Field Security by Role

You also can set up field security for all users that are assigned to a specific role.

- 1 Assign users to roles in Role Membership Maintain (36.3.6.6.1).
- 2 Execute Field Security by Role (36.3.15.2). This function adds all users who belong to a specified role or roles to the list of authorized users for a validated field.

Fig. 7.1
Field Security by Role (36.3.15.2)



The screenshot shows a software window titled "Field Security by Role". It features a menu bar with options: "Go To", "Actions", "Copy", "Print", and "Preview". Below the menu bar, there are three input fields: "Field Name:", "Role Name:", and "Comments:". The "Field Name:" field is the largest and is currently empty. The "Role Name:" field is smaller and also empty. The "Comments:" field is the smallest and is empty.

Even with this process, field security is only available at the user level, not the role level. Field Security by Role is simply a batch utility that lets you add multiple users simultaneously. This has the following consequences:

- If you remove a user from a role that was given access to a field, that user can still access the field. To prevent this, use Field Security Maintenance (36.3.15.1) to remove the individual user.
- You cannot use Field Security by Role to remove multiple users from the list of authorized users. To remove multiple users, you must remove users individually in Field Security Maintenance.
- If you delete a role in Role Delete (36.3.6.4), individual records remain on the system until you delete them in Field Security Maintenance.

Once Field Security by Role is executed for a field and role, all users who belong to the role display in Field Security Maintenance as authorized to access the field. The Comments field in Field Security by Role displays as the comment for the field and user combination in Field Security Maintenance.

Controlling Inventory Updates

The system has two ways to control inventory updates within a domain. Updates can be controlled by:

- Sites within a domain
- Specific combinations of inventory-related fields such as item number and location

Note If you are using the optional QAD Warehousing module, you can also assign security by warehouse using Warehouse Security Maintenance (4.23.13).

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.

Note By default, users have access to all sites unless security has been defined in this program.

Access is managed by user and role. A user can access a site only if that user's ID or role is specified in the User IDs/Roles field in Site Security Maintenance (36.3.13.8). Use Site Security Report (36.3.13.9) to view site security defined for system users.

Fig. 7.2
Site Security Maintenance (36.3.13.8)

When a user enters a restricted site code in a site-controlled program, the system checks the value of the User IDs/Roles field associated with the site in Site Security Maintenance. If the user does not belong to an appropriate role, or if 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 QM Quality Management Control (19.26.24) do not use site security.
- You must set up each domain individually.

Implementing Site Security

It is important to plan site security carefully and to follow closely the procedures for creating roles, users, and associations between users and roles. After you have created any site security records, users who are not listed individually or who have not been assigned access privileges in Site Security Maintenance (36.3.13.8) cannot complete transactions at secured sites.

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 to which you do not have access, 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.

Update Restrictions

You can use Site Security Maintenance to specify which roles are allowed to update inventory at particular sites within a domain. This type of security is discussed in the section “Access by Site” on page 112.

However, when stringent internal controls for regulatory reporting exist, you may need to control who can update inventory at a more detailed level than the site. For example, you might need to allow only certain roles to transfer inventory out of a Quarantine location, or restrict certain roles from making specific inventory status code changes within a site.

You can use the programs on the Update Restrictions Menu to implement stricter control over inventory movements and status updates that are completed throughout the system. Each particular update restriction program affects a set of programs where inventory transactions occur. Grouping the transactions this way lets you focus control on the areas that are critical to your business practices.

The specific combination of fields that you use to manage inventory depends on the particular program that supports the update restriction, but can include item number, site, location, inventory status code, and the GL account affected by the transaction.

Using the features of Update Restrictions, you can:

- Authorize a role to maintain records, create transactions, or change inventory status for specific item, site, and location combinations in a set of programs that create transactions.
- Restrict a role from maintaining records, creating transactions, or changing inventory status for specific item, site, and location combinations in certain system programs.
- Generate a report of all defined update restrictions.

You should define update restrictions as part of a general security model, which includes defining roles for your organization, as well as setting up any required site and field security. The system applies site and field security before update restrictions.

Note The descriptions of the programs in this section only discuss fields that are unique to that program. The item, number, site, and location fields operate identically in each program.

Setting Up Update Restrictions

You can set up update restrictions for the following types of functions. “General Rules for Update Restrictions” on page 115 describes the common logic used in all of the functions to determine whether restrictions apply to a user’s role.

- Inventory transfers. See “Inventory Transfer Restriction Maintenance” on page 116 for details.
- Inventory details. See “Inventory Detail Restriction Maintenance” on page 117 for details.
- Issues and receipts. See “Unplanned Issue/Receipt Restriction Maintenance” on page 118 for details.
- Maintaining all types of purchase orders. See “PO Restriction Maintenance” on page 119 for details.
- Receipt handling and status change. See “PO Receipts Restriction Maintenance” on page 120 for details.
- Maintaining sales order, invoice, and quote lines. See “SO Restriction Maintenance” on page 120 for details.
- Creating shipments and maintaining shippers. See “SO Shipments Restriction Maintenance” on page 121 for details.
- Maintaining distribution orders (DO). See “DO Restriction Maintenance” on page 121 for details.
- Creating DO shipments. See “DO Shipments Restriction Maintenance” on page 122 for details.
- Creating DO receipts. See “DO Receipts Restriction Maintenance” on page 122 for details.
- Maintaining records, creating receipts, and completing shipments in SSM. See “SSM Restriction Maintenance” on page 122 for details.

Update restrictions only apply to the domain where they are defined. If no restrictions are defined, all roles with access to these programs can perform data updates, as long as they also have access to the site being updated.

Using Wild Cards for Update Restrictions

You can enter item number, site, location, and status values using wild cards. Use the asterisk (*) and exclamation point (!) as inclusion and exclusion wild cards respectively:

- * indicates access to all.
- string* indicates access to all beginning with string.
- string indicates access to that string only.
- !string* indicates access is restricted from all beginning with that string.
- !string indicates access is restricted from that string only.

Use combinations of inclusive and exclusive restrictions to specify both large and small sets of value combinations.

General Rules for Update Restrictions

- 1 If one restriction is set up, all transactions are validated and have to pass to be accepted. If no restrictions are set up, all transactions are accepted.
Example As soon as a restriction is set up in Inventory Restriction Detail Maint (36.3.7.2), then Inventory Detail Maintenance (3.1.1) is secured for all transactions.
- 2 Defining a record in one of the restriction setup programs only affects the programs covered by this restriction. For example, defining a restriction in Inventory Restriction Detail Maint has no effect on Sales Order Maintenance because Sales Order Maintenance restrictions are specified in SO Restrictions Maintenance (36.3.7.8).
- 3 The values from the transaction are matched against the restrictions defined. There has to be one positive match for the transaction to be accepted.
- 4 If there is more than one match, all must be positive matches for the transaction to be accepted. In other words, the first negative match will make the transaction fail.
- 5 There is an implied hierarchy within the fields used to set up the restrictions (Item, Site, Location, and so on). The hierarchy is the order in which they appear on the screen where the restrictions are set up. If a transaction matches a field value that is excluded for a role—for example, Site: !10000—the system fails the transaction without considering the values of the fields lower in the setup screen.
- 6 These rules are the same for all transactions that are enabled for this functionality. The fields may be different from one transaction to another, but the above rules still apply.

Examples of Update Restrictions

The examples in this section relate to Inventory Transfer Restriction Maintenance. However, as the programs on the Update Restrictions Menu all operate in a similar manner, these examples are relevant to the other Update Restrictions programs.

Example For the specified role, one restriction is defined for a combination of values:

Role (Stock), Item (22-100), From Site (10000), To Site (11000), From Location (100), To Location (200), From Status (20), To Status (20)

Only users with the Stock role can create transactions for this combination of values. This role cannot create transactions for any other combinations; no other role can create transactions for any combinations at all.

Example For the specified role, restrictions are defined for multiple items:

Item (22-1*), From and To Site (10000), From and To Location (100), From and To Status (*)
Item (22-2*), From and To Site (11000), From Location (100), To Location (200), From and To Status (*)

With these restrictions defined, only the specified role can create transactions for items with any status where:

From and To Site is 10000, From and To Location is 100, and item numbers begin with 22-1
From and To Site is 11000, From Location is 100, To Location is 200, and item numbers beginning with 22-2

No other role can create transactions for any combinations at all.

Example When users will be prevented from creating transactions for items with only a few combinations of values, it is best to first define restrictions that allow all changes; then define additional restrictions for the small set of value combinations where changes are prevented.

For each role, set access to all (*) for all items, sites, locations, and statuses; then set the further restrictions:

Item (*), From Site (*), To Site (*), From Location (*), To Location (*), From Status (*), To Status (*)

Item (!22-200*), From Site (10000), To Site (10000), From Location (100), To Location (200), From Status (*), To Status (*)

For each role where these restrictions are defined, they prevent transfers from location 100 to 200 for items that begin with 22-200 in site 10000. Transfers are still allowed for items with all other value combinations.

Inventory Transfer Restriction Maintenance

Use Inventory Transfer Restriction Maintenance (36.3.7.1) to specify role-based restrictions on inventory transfers in the following programs:

- Transfer – Single Item (3.4.1)
- Transfer – Multi Item (3.4.2)
- Transfer with Lot/Serial Change (3.4.3)
- Batchload Transfer with Lot/Serial Change (3.4.4)

For each item, restrictions are based on combinations of values for From and To sites, locations, and inventory statuses. All fields are required.

Fig. 7.3

Inventory Transfer Restriction Maintenance (36.3.7.1)

Role. Enter the name of a role defined in your system.

Use roles to streamline security setup. When a new user record is created, you assign the user a role to ensure they have correct access.

Item Number. Enter the code identifying an inventory item defined in Item Master Maintenance (1.4.1).

Item codes uniquely identify items or products. These may be raw materials, purchased or manufactured intermediates, finished items, or packaging materials. Item codes are also used to identify planning items, configured products, repair parts, service items, and kits.

Most reports and inquiries can be selected by item number.

Site. Enter the originating site that is part of the definition for this update restriction.

To. Enter the receipt or receiving site that is part of the definition for this update restriction.

Location. Enter the originating location that is part of the definition for this update restriction.

To. Enter the receipt or receiving location that is part of the definition for this update restriction.

Inventory Status. Enter the original or starting status code that is part of the definition for this inventory restriction.

Restrictions can specify whether this status code can be changed to another specified status code or whether it can be changed at all. This is part of a restriction definition that specifies which roles have access to update specific combinations of items, sites, and locations.

Define status codes in Inventory Status Code Maintenance (1.1.1). Assign inventory status codes to sites with Site Maintenance (1.1.13) and locations with Location Maintenance (1.1.18). Optionally assign default inventory status codes for purchase order or work order receipts to individual items using Item Master Maintenance (1.4.1), Item Inventory Data Maintenance (1.4.5), or Item-Site Inventory Data Maintenance (1.4.16).

To. Enter the destination or target status code that is part of the definition for this inventory restriction.

Inventory Detail Restriction Maintenance

Use Inventory Detail Restriction Maintenance (36.3.7.2) to specify role-based restrictions on updating inventory details in these programs:

- Inventory Detail Maintenance (3.1.1)
- Detail Maintenance by Item/Lot (3.1.2)

Multiple To statuses can be specified for each site, location, and From status combination for an item. Select the Change Inventory Status check box and press Next; this displays the Valid Inventory Status Code frames for maintaining the list of valid To statuses. Enter a status code in the bottom frame and press Next to add it to the list of valid codes.

If the Change Inventory Status is not selected, the system deletes the list of valid To status codes defined for the current role, item, and values combination.

Fig. 7.4
Inventory Detail Restriction Maintenance (36.3.7.2)

Change Inventory Status. Indicate how you want this update restriction to apply to inventory status changes:

Not selected: Users can change other inventory details such as assay percentage and expire date but they cannot change the inventory status.

Selected: Users can modify the inventory status associated with records for the specified combination of item, site, and location as long as they select an inventory status associated with this restriction.

Selecting the check box displays the list of target status codes that are allowed and lets you add or remove codes as required.

Status Code. Enter a status code to add to the list of valid target status codes that the current code can be changed to. The list is part of an update restriction defined for a particular role and combination of item, site, and location.

Unplanned Issue/Receipt Restriction Maintenance

Use Unplanned Issue/Receipt Restriction Maintenance (36.3.7.3) to define role-based restrictions on issues and receipts in these programs:

- Issues–Unplanned (3.7)
- Receipts–Unplanned (3.9)
- Receipts–Sales Order Return (3.10)
- Receipts–Return to Stock (3.11)
- Receipts–Backward Exploded (3.12)

Fig. 7.5
Unplanned Issue/Receipt Restriction Maintenance (36.3.7.3)

Account. Enter a GL account code as part of an issues and receipts update restriction defined for a particular role and combination of item, site, and location.

The account number is used when applying update restrictions to programs such as Issues–Unplanned (3.7) and Receipts–Unplanned (3.9). Define account codes in Account Create (25.3.13.1).

Sub-Account. Enter a GL sub-account code as part of an issues and receipts update restriction defined for a particular role and combination of item, site, and location.

The account number is used when applying update restrictions to programs such as Issues–Unplanned (3.7) and Receipts–Unplanned (3.9). Define sub-accounts in Sub-Account Create (25.3.17.1).

Cost Center. Enter a cost center code as part of an issues and receipts update restriction defined for a particular role and combination of item, site, and location.

The account number is used when applying update restrictions to programs such as Issues–Unplanned (3.7) and Receipts–Unplanned (3.9). Define cost centers in Cost Center Create (25.3.20.1).

Project. Enter a project code as part of an issues and receipts update restriction defined for a particular role and combination of item, site, and location.

The account number is used when applying update restrictions to programs such as Issues–Unplanned (3.7) and Receipts–Unplanned (3.9). Define projects in Project Create (25.3.11.1.1).

PO Restriction Maintenance

Use PO Restriction Maintenance (36.3.7.5) to specify role-based restrictions on maintaining orders in these programs:

- Build PO from Requisitions (5.2.18)
- Blanket Order Maintenance (5.3.1)
- Blanket Order Release to PO (5.3.6)
- Scheduled Order Maintenance (5.5.1.13)
- Purchase Order Maintenance (5.7)

Fig. 7.6

PO Restriction Maintenance (36.3.7.5)

PO Receipts Restriction Maintenance

Use PO Receipts Restriction Maintenance (36.3.7.6) to specify role-based receipt handling and status change restrictions in these programs:

- Purchase Order Receipts (5.13.1)
- Purchase Order Returns (5.13.7)
- PO Shipper Maintenance (5.13.14)
- PO Fiscal Receiving (5.13.16)
- PO Shipper Receipt (5.13.20)

Multiple To statuses can be specified for each site, location, and From status combination for an item. Select the Change Inventory Status check box and press Next; this displays the Valid Inventory Status Code frames for maintaining the valid To status codes. Enter a status code in the bottom frame and press Next to add it to the list of valid codes.

If the Change Inventory Status check box is not selected, the system deletes the list of valid To status codes defined for the current role, item, and value combination.

Fig. 7.7

PO Receipts Restriction Maintenance (36.3.7.6)

SO Restriction Maintenance

Use SO Restriction Maintenance (36.3.7.8) to specify role-based restrictions on maintaining sales order, invoice, and quote lines in these programs:

- SO Maintenance (7.1.1)
- Scheduled Order Maintenance (7.3.13)
- Pending Invoice Maintenance (7.13.1)

- Sales Quote Maintenance (7.12.1)
- Sales Quote Copy from Order (7.12.5)
- Sales Quote Copy from Quote (7.12.6)
- Sales Quote Release to Order (7.12.10)

Fig. 7.8

SO Restriction Maintenance (36.3.7.8)

SO Shipments Restriction Maintenance

Use SO Shipments Restriction Maintenance (36.3.7.9) to specify role-based restrictions on creating shipments and maintaining shippers in these programs:

- Picklist/Pre-Shipper – Automatic (7.9.1)
- Pre-Shipper/Shipper Workbench (7.9.2)
- Pre-Shipper/Shipper Confirm (7.9.5)
- Pre-Shipper/Shipper Auto Confirm (7.9.7)
- Sales Order Shipper Maintenance (7.9.8)
- Sales Order Shipments (7.9.15)
- Shipper Unconfirm (7.9.21)

Fig. 7.9

SO Shipments Restriction Maintenance (36.3.7.9)

DO Restriction Maintenance

Use DO Restriction Maintenance (36.3.7.13) to specify role-based restrictions on maintaining distribution orders (DOs) in these programs:

- Distribution Order Workbench (12.17.13)
- Distribution Order Maintenance (12.17.14)
- Distribution Order Processing (12.17.21)

Fig. 7.10
DO Restriction Maintenance (36.3.7.13)

DO Shipments Restriction Maintenance

Use DO Shipments Restrictions Maintenance (36.3.7.14) to specify role-based restrictions on creating shipments in these programs:

- Distributed Order Processing (12.17.21)
- Distributed Order Shipments (12.17.22)

Fig. 7.11
DO Shipments Restriction Maintenance (36.3.7.14)

DO Receipts Restriction Maintenance

Use DO Receipts Restriction Maintenance (36.3.7.15) to specify role-based restrictions on creating DO receipts in these programs:

- Intersite Request Maintenance (12.15.1)
- Distributed Order Receipt (12.15.20)

Fig. 7.12
DO Receipts Restriction Maintenance (36.3.7.15)

SSM Restriction Maintenance

Use SSM Restriction Maintenance (36.3.7.17) to specify role-based restrictions on maintaining records and creating receipts and shipments for RMAs, RTSs, and MOs in these programs:

- RMA Maintenance (11.7.1.1)

- RMA Receipts (11.7.1.13)
- RMA Shipments (11.7.1.16)
- RTS Maintenance (11.7.3.1)
- RTS Receipts (11.7.3.13)
- RTS Shipments (11.7.3.16)
- Material Order Maintenance (11.11.1)
- Material Order Shipments (11.11.6)
- MO Direct/Pending Returns (11.11.8)

Fig. 7.13
SSM Restriction Maintenance (36.3.7.17)

Defining GL Account Security

Using GL account security, you can restrict who can create transactions in operational functions that update GL accounts based on user ID or role.

Use GL Account Security Maintenance (36.3.13.1) to assign users or roles to account numbers. Use the GL Account Security Report (36.3.13.2) to list all accounts that have controlled access.

Fig. 7.14
GL Account Security Maintenance (36.3.13.1)

When a user attempts to create an operational transaction affecting an account, the system checks to see if account security is defined. If it is, the system verifies that the user ID and roles associated with the user are found on the list associated with the account. If a match is not found, a message displays and the user cannot complete the transaction.

If no account security has been defined, all users and roles are permitted to update the account, within the parameters of other restrictions.

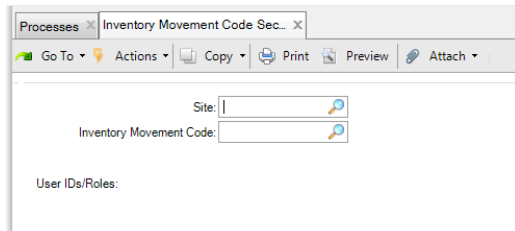
Note Account security is not applied during Operational Transaction Post (25.13.7) or Invoice Post and Print (7.13.4). Use Role Permissions Maintain to restrict posting functions.

Defining Inventory Movement Code Security

Use Inventory Movement Code Security (36.3.13.13) to grant or deny access to individuals and roles to shipping transactions that reference a specific inventory movement code at a particular site.

Fig. 7.15

Inventory Movement Code Security (36.3.13.13)

The screenshot shows a web application window with a title bar containing 'Processes' and 'Inventory Movement Code Sec...'. Below the title bar is a menu bar with options: 'Go To', 'Actions', 'Copy', 'Print', 'Preview', and 'Attach'. The main content area has two input fields: 'Site:' and 'Inventory Movement Code:', each with a search icon to its right. Below these fields is a label 'User IDs/Roles:'.

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. For more information on movement codes, see [QAD Sales User Guide](#).

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.

Use Inventory Movement Code Security Browse (36.3.13.14) to display inventory movement code security records. You can view fields associated with a record 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.

Segregation of Duties

This section describes how to configure and set up segregation of duties. Segregation of duties is an internal control that prevents a single user from performing two or more phases of a transaction or operation.

Overview 127

Explains the purpose of segregation of duties, including usage examples. Introduces key segregation of duties concepts.

Plan a Segregation of Duties System 131

Outlines how to plan your segregation of duties system by creating a high-level overview of your business environment.

Segregation of Duties Rule Checking 132

Discusses the role permissions and role membership rules that segregation of duties enforces.

Complete Prerequisite Activity 138

Describes the prerequisites that must be met before you can implement segregation of duties.

Activate Segregation of Duties 138

Describes how to activate segregation of duties and how to block any changes to role-based security that would allow users to access conflicting resources.

Maintain Segregation of Duties Categories 140

Outlines how to create, modify, view, and delete segregation of duties categories.

Assign Resources to Segregation of Duties Categories 142

Describes how to associate an application resource with a segregation of duties category.

Maintain the Segregation of Duties Matrix 144

Discusses how to define the compatibility of segregation of duties categories.

Define Role Permissions 148

Outlines how the associations between roles and functions are constrained by segregation of duties policy.

Define Role Membership 148

Describes how the associations between users and roles are constrained by segregation of duties policy.

Maintain Segregation of Duties Policy Exceptions 149

Discusses segregation of duties policy exceptions, which provide a specified user with access to a pair of resources that are not compatible under segregation of duties policy.

Segregation of Duties Role Exclusions 150

Outlines how you can specify that a particular role is exempt from segregation of duties rule checks and blocking.

Import and Export Segregation of Duties Data 151

Describes how you can create and load default data for segregation of duties categories, matrices, and resource assignments using Excel and XML.

Report and View Logs and Violations 158

Lists the reports and views that let you review segregation of duties violations.

Archive Log Record Files 162

Discusses how to archive log records when an online history of segregation of duties violations is no longer needed.

Overview

Corporate governance legislation, such as the Sarbanes-Oxley Act of 2002, demands that organizations introduce stronger internal controls into their business processes. Among these internal controls is segregation of duties.

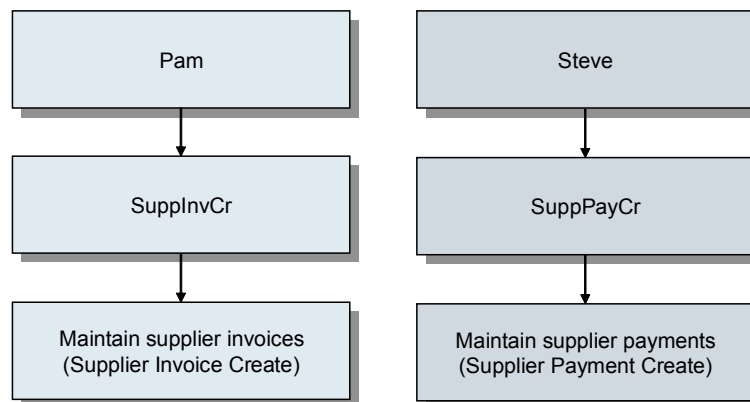
Segregation of duties refers to the notion that the duties of individuals in an organization should be limited to certain areas of responsibility, so as to minimize the ability of any individual to misappropriate company property. Segregation of duties prevents a single user from performing two or more phases of a transaction or operation. See “Segregation of Duties Verification” on page 128 for an introduction to the rules on which segregation of duties is based.

If a person can commit and conceal errors, irregularities, or both while performing day-to-day activities, they have generally been assigned or allowed access to incompatible duties or responsibilities.

The ability to automate and report on internal controls, such as segregation of duties, reduces the likelihood of non-compliance to corporate governance regulations and also reduces compliance-related costs.

Figure 8.1 shows the separation of business functions within an organization that enforces segregation of duties. Pam is responsible for maintaining supplier invoices and has been assigned the SuppInvCr role. All users assigned this role can create supplier invoices using Supplier Invoice Create.

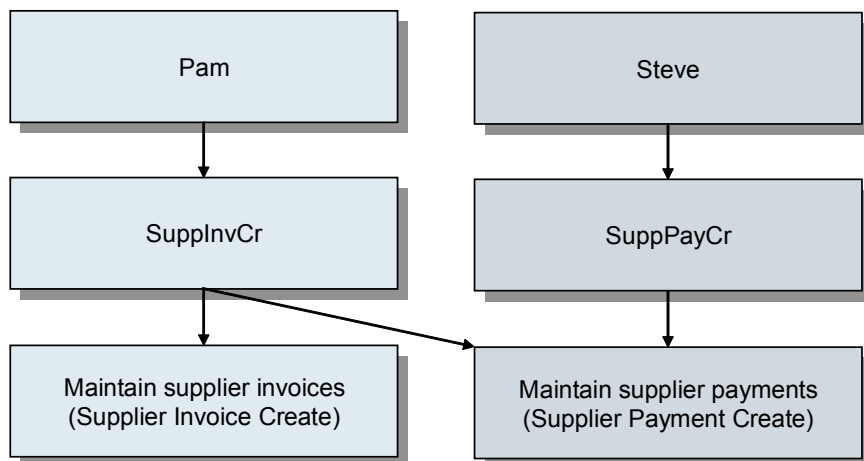
Fig. 8.1
Segregation of Duties Example



Steve is responsible for creating supplier payment records and is assigned to the SuppPayCr role. All users assigned this role can create and modify supplier payments; however, they cannot maintain supplier invoices since this ability would violate segregation of duties policy.

Figure 8.2 shows the business functions within an organization that has not implemented segregation of duties, or which has permitted a known segregation of duties violation. In this example, users assigned the SuppInvCr role can create supplier payments as well as create supplier invoices.

Fig. 8.2
Segregation of Duties Violation



Segregation of duties is achieved in the system by assigning application resources to a finite number of user-defined segregation of duties categories. A *segregation of duties category* is a way of grouping compatible system activities.

Setting up segregation of duties in your system is optional. However, the decision whether or not to use segregation of duties should be considered first in your security implementation planning. For details, see “Implementation Summary” on page 6.

Segregation of Duties Verification

The system verifies the integrity of your defined segregation of duties policy by ensuring that the following two rules are not violated:

- Rule 1 verifies that the assignments specified do not violate role permissions compliance; that is, all the resources to which a role grants access must be associated with compatible segregation of duties categories.
- Rule 2 verifies that the assignments specified do not violate role membership compliance; that is, all roles to which a user belongs must be associated with compatible segregation of duties categories.

Each system user is logically associated with a set of segregation of duties categories, indirectly, through the user’s role assignment.

The SOD Block All Rule Violations field in SOD Configuration (36.3.27.14) controls whether the system should block any changes to role-based security that would allow users to access conflicting resources. If this field is cleared, administrators are not blocked from providing users with access to functions with conflicting segregation of duties categories. However, a violation is raised and written to the segregation of duties logs.

Important In the context of this chapter, the term administrator refers to the user who maintains a company’s security settings.

See “Segregation of Duties Rule Checking” on page 132 for detailed information.

Segregation of Duties Compatibility Matrix

When segregation of duties categories are defined within the system, you specify which segregation of duties categories are mutually exclusive. Segregation of duties compatibility constraints are stored in the system as pairs in a segregation of duties category matrix.

If two categories are compatible, a single user is permitted to have access to application resources that exist in both of these categories without violating a defined segregation of duties policy. Conversely, if two categories are incompatible, a single user is permitted to have access to a function in either category, but not both.

To ensure that segregation of duties provides adequate internal control within your organization, a user cannot have access privileges to any functions that belong to mutually exclusive categories.

See “Maintain the Segregation of Duties Matrix” on page 144.

Segregation of Duties Policy Exceptions

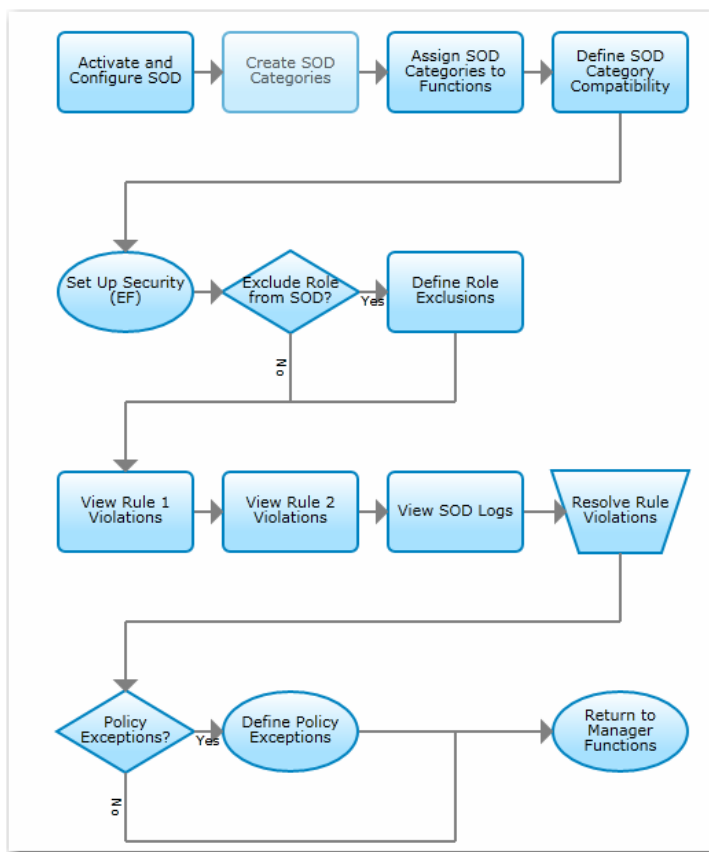
Segregation of duties permits policy exceptions to be defined to accommodate special circumstances—for example, when a business unit lacks sufficient personnel to adequately implement segregation of duties. Policy exceptions are defined on a user-by-user basis. That is, individual users can be given access to resources that are not compatible under your segregation of duties policy.

See “Maintain Segregation of Duties Policy Exceptions” on page 149.

Segregation of Duties Process Workflow

Use the programs in the Segregation of Duties Menu to set up and configure segregation of duties functions. Figure 8.3 illustrates one possible segregation of duties process workflow; use it to set up segregation of duties functions in your environment.

Fig. 8.3
Segregation of Duties Setup Flow



The process of setting up segregation of duties incorporates several steps—defining role permissions and role membership, for example—that are required to configure a system regardless of whether segregation of duties is implemented. However, once application resources have been associated with a segregation of duties category, the role permissions that can be defined are constrained by your segregation of duties policy. For this reason, you should carefully consider the need to implement segregation of duties and plan accordingly. See “Plan a Segregation of Duties System” on page 131. For details on planning and implementing security in your system, see “Implementation Summary” on page 6.

After you create user records in User Maintenance (36.3.1) and define roles in your system in the Role function, the first activity is to activate segregation of duties using SOD Configuration (36.3.27.14) and specify segregation of duties configuration settings. See “Activate Segregation of Duties” on page 138.

When segregation of duties is activated, you should then define the segregation of duties categories using SOD Category Create (36.3.27.1.1). For each category, you specify a unique category code and a description. See “Maintain Segregation of Duties Categories” on page 140.

After defining your segregation of duties categories, the next step is to associate an application resource with a segregation of duties category by using SOD Category Membership Maintain (36.3.27.4). See “Define Role Permissions” on page 148.

Use SOD Matrix Maintain (36.3.27.3) to define the segregation of duties categories that are mutually exclusive. Segregation of duties compatibility constraints are stored in the system as pairs in a segregation of duties category matrix. See “Maintain the Segregation of Duties Matrix” on page 144.

The next step is to define role permissions in your system. This associates application resources to user roles. See “Define Role Permissions” on page 67. This step is now constrained by the segregation of duties policy you have defined.

Next define your role membership. This step associates users with roles and—as with the previous step—is constrained by the defined segregation of duties policy.

If you implement segregation of duties in a new database and set up segregation of duties categories, compatibilities, and exclusions before setting up roles, segregation of duties would prevent you from assigning two incompatible roles to a user.

To allow for situations where a technical user account—for example, an integration user—needs access to all system functions, you can define roles that are exempt from segregation of duties rules using SOD Role Exclusion (36.3.27.8). See “Segregation of Duties Role Exclusions” on page 150.

To accommodate situations—a staff shortage, for example—where a user might need to participate in more than one part of a business process, you can define segregation of duties policy exceptions by using SOD Policy Exception Create (36.3.27.2.1). See “Maintain Segregation of Duties Policy Exceptions” on page 149.

Use the SOD Violations report (36.3.27.9) and SOD Log Viewer (36.3.27.6) to view current segregation of duties policy violations and a violations history file, respectively. See “Report and View Logs and Violations” on page 158.

Segregation of duties violations that arise during segregation of duties maintenance are recorded in a log. Use SOD Log Archive (36.3.27.7) to archive log table records. See “Archive Log Record Files” on page 162.

Plan a Segregation of Duties System

Every business environment has unique segregation of duties requirements. You may find it helpful to create a high-level overview of your business environment and use a top-down approach when defining your segregation of duties requirements.

QAD delivers a set of default roles and segregation of duties categories that facilitate the implementation of segregation of duties. You can load the default segregation of duties data using SOD Import/Export (36.3.27.15). See “Import and Export Segregation of Duties Data” on page 151.

Before you begin to set up segregation of duties functions, consider creating:

- A detailed segregation of duties plan including details such as:
 - A detailed list of your roles and their business responsibilities
 - A detailed list of resources that are in conflict
 - A detailed list of the associations required between application resources, segregation of duties category code, and role

- A detailed list of the segregation of duties policy exceptions required
- A maintenance schedule for planning when, and under what conditions, your segregation of duties policy will be reviewed and changes implemented
- An information retention plan detailing how long segregation of duties-related information, such as log files, are kept online for reporting purposes
- An archive plan detailing when segregation of duties log records are archived and where they are stored
- A detailed segregation of duties plan that describes how the business functions within your system will be segregated according to roles

Consider the following points:

- Legislation such as the Sarbanes-Oxley Act is designed toward achieving transparency of disclosure, integrity of business operations, and financial accountability for accurate reporting. As such, this may require your organization to comply with specific and stringent electronic information retention regulations. Make sure you are familiar with the impact such legislation has on your specific industry or region.
- Completing the segregation of duties setup correctly the first time will help to minimize the number of segregation of duties policy conflicts that will require corrective action. Also, closely monitor any changes that must be applied to your segregation of duties setup.
- To minimize the number of potential segregation of duties conflict violations in your system, try to define as few constraints—that is, the number of incompatible categories in your system—as possible.

Segregation of Duties Rule Checking

Role Permissions Validation

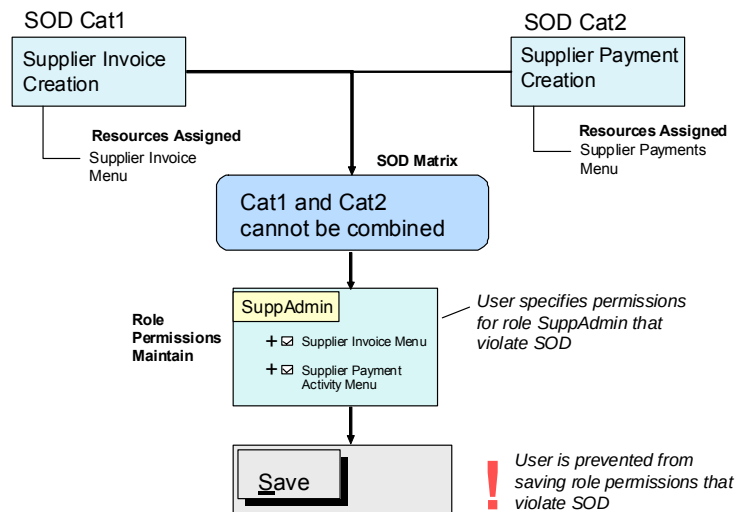
When you add a resource to the list of resources allowed for a role in Role Permissions Maintain (36.3.6.5), the system validates the assignment to verify that all the role resources belong to compatible segregation of duties categories (Rule 1 validation). If Rule 1 is violated, the system blocks the role permissions updates, and returns an error message indicating the cause of the violation.

When you add a resource to the list of resources allowed for a certain role, the system also checks that roles to which a user belongs are associated with compatible segregation of duties categories (Rule 2 validation). If Rule 2 is violated, the system displays a warning and saves the change. However, an entry is created in the segregation of duties log.

Note When the SOD Block All Rule Violations field is selected in SOD Configuration (36.3.27.14), the system blocks Rule 2 violations in Role Permissions Maintain (36.3.6.5) instead of issuing a warning.

When a resource is removed from the list of resources allowed for a role, the system runs the Rule 1 and Rule 2 validation. The validation is run before and after the deletion to detect if an existing violation has been solved by removing the resource. A new entry is written to the segregation of duties log if the deletion fixes an existing violation.

Fig. 8.4
Role Permissions Validation



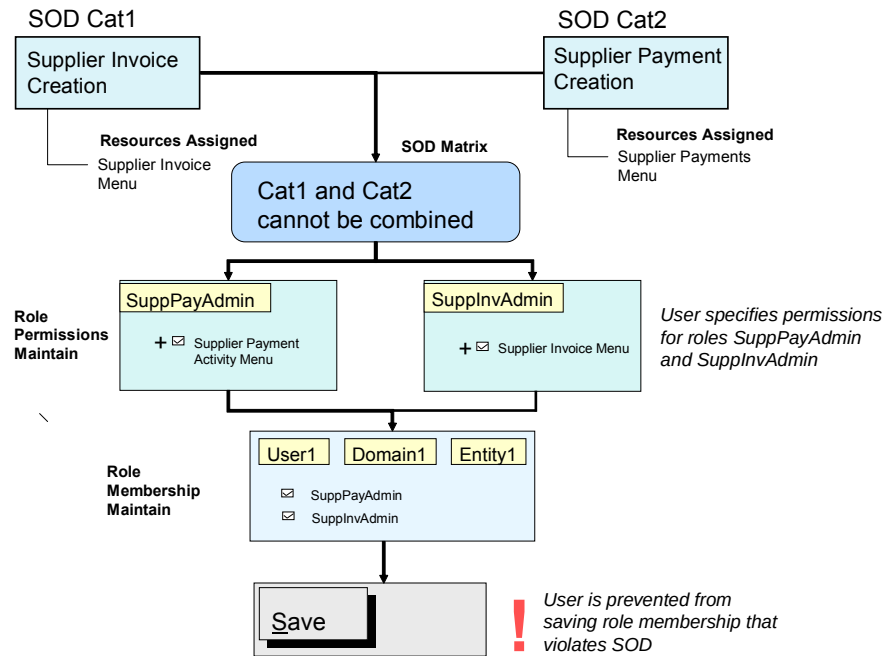
Role Membership Validation

When a user is added to a role using Role Membership Maintain (36.3.6.6), the system runs checks to validate that the roles to which the user belongs to have compatible segregation of duties categories (Rule 2 validation). If the roles have incompatible segregation of duties categories and Rule 2 is violated, the system blocks the role membership update and displays an error.

If you remove a user from a role, the system runs checks before and after the update to determine the status of role membership violations. If the deletion fixes an existing violation, the system creates entries in the segregation of duties log to reflect this.

When the SOD Block All Rule Violations field is selected in SOD Configuration (36.3.27.14), you are blocked from performing steps that violate role membership compatibility.

Fig. 8.5
Role Membership Validation



Direct and Indirect Violations

A direct segregation of duties violation occurs when you attempt to use Role Permissions Maintain (36.3.6.5) to assign a role to functions that have incompatible segregation of duties categories. Direct violations also occur if you attempt to use Role Membership Maintain (36.3.6.6) to assign multiple roles to a user that have incompatible segregation of duties categories.

Users are always blocked from performing actions in Role Permissions Maintain (36.3.6.5) that cause Rule 1 violations and are always blocked from performing actions in Role Membership Maintain (36.3.6.6) that cause Rule 2 violations, regardless of the setting in the SOD Block All Rule Violations field in SOD Configuration (36.3.27.14).

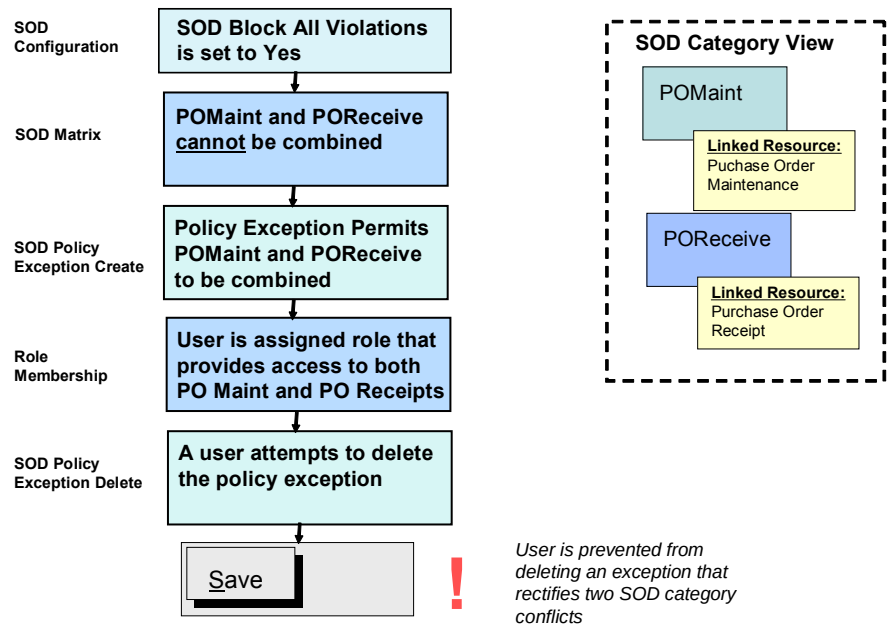
Indirect violations occur if you perform actions that violate segregation of duties rules using screens other than Role Permissions Maintain (36.3.6.5) and Role Membership Maintain. However, role membership (Rule 2) violations caused by updates in Role Permissions Maintain (36.3.6.5) are also examples of indirect violations.

Figure 8.6 shows how the system handles an indirect violation when the SOD Block All Violations field is selected in SOD Configuration (36.3.27.14). In this example, the segregation of duties category code POMaint applies to the creation of purchase orders (POs) in Purchase Order Maintenance, and the segregation of duties category code POReceive applies to the recording of PO receipts in Purchase Order Receipts. For segregation of duties to be properly implemented, the PO maintenance and PO receipt functions must be performed by two different users. The POMaint and POReceive categories are defined as mutually exclusive in SOD Matrix Maintain (36.3.27.3).

The user who maintains POs has to take personal leave unexpectedly and the PO receipt clerk has to perform both duties for a number of days. A segregation of duties policy exception is defined for this, and the PO maintenance role is assigned to the PO receipts clerk. The assignment of both roles violates segregation of duties rules, but because of the policy exception, no violations are raised.

A user attempts to delete the segregation of duties policy exception, but is blocked from doing so. Deleting the exception causes indirect segregation of duties violations.

Fig. 8.6
Indirect Segregation of Duties Violation



Segregation of Duties Rule Matrix

Table 8.1 lists user actions and describes how the system reacts to these actions if segregation of duties is disabled, if segregation of duties is enabled, but SOD blocking is disabled, and if both segregation of duties and SOD blocking are enabled.

Table 8.1
Segregation of Duties Rule Matrix

Action	Segregation of Duties Inactive	Segregation of Duties Active, SOD Blocking Disabled	Segregation of Duties Active, SOD Blocking Enabled
You add a resource to a role in Role Permissions Maintain (36.3.6.5), causing violations.	No segregation of duties checking.	Rule 1: Runs segregation of duties violation checks. The action is blocked. Rule 2: Runs segregation of duties violation checks. The action is not blocked and the violation is logged.	Rule 1: Runs segregation of duties violation checks. The action is blocked. Rule 2: Runs segregation of duties violation checks. The action is blocked.
You remove a resource that caused violations from a role in Role Permissions Maintain (36.3.6.5).	No segregation of duties checking.	Rule 1: Validates segregation of duties violation checks. The previous violation is fixed. Rule 2: Validates segregation of duties violation checks. The previous violation is fixed.	Not applicable.
You add a user to a role in Role Membership Maintain (36.3.6.6), causing violations.	No segregation of duties checking.	Rule 2: Runs segregation of duties violation checks. The action is blocked.	Rule 2: Runs segregation of duties violation checks. The action is blocked.
You remove a user that caused violations from a role in Role Membership Maintain (36.3.6.6).	No segregation of duties checking.	Rule 2: Runs segregation of duties violation checks. The previous violation is fixed.	Not applicable.
You add a resource to a segregation of duties category, causing violations.	No segregation of duties checking.	Rule 1: Runs segregation of duties violation checks. The action is not blocked and the violation is logged. Rule 2: Runs segregation of duties checks. The action is not blocked and the violation is logged.	Rule 1: Validates segregation of duties violation checks. The action is blocked. Rule 2: Validates segregation of duties violation checks. The action is blocked.
You remove a resource that caused violations from a segregation of duties category in SOD Category Membership Maintain (36.3.27.4).	No segregation of duties checking.	Rule 1: Runs segregation of duties violation checks. The previous violation is fixed. Rule 2: Runs segregation of duties violation checks. The previous violation is fixed.	Not applicable.
You define an incompatibility in SOD Matrix Maintain (36.3.27.3).	No segregation of duties checking.	Rule 1: Runs segregation of duties violation checks. The action is not blocked and the violation is logged. Rule 2: Runs segregation of duties checks. The action is not blocked and the violation is logged.	Rule 1: Runs segregation of duties violation checks. The action is blocked. Rule 2: Runs segregation of duties violation checks. The action is blocked.

Action	Segregation of Duties Inactive	Segregation of Duties Active, SOD Blocking Disabled	Segregation of Duties Active, SOD Blocking Enabled
You delete an incompatibility in SOD Matrix Maintain (36.3.27.3).	No segregation of duties checking.	Rule 1: Runs segregation of duties violation checks. The previous violation is fixed. Rule 2: Validates segregation of duties violation checks. The previous violation is fixed.	Not applicable.
You define an exception in SOD Policy Exception Create (36.3.27.2.1) that rectifies an existing violation.	No segregation of duties checking.	Rule 1: Validates segregation of duties violation checks. The previous violation is fixed. Rule 2: Validates segregation of duties violation checks. The previous violation is fixed.	Not applicable.
You delete an exception in SOD Policy Exception Delete (36.3.27.2.4). The policy exception had caused a previous violation to be resolved, and is now deleted.	No segregation of duties checking.	Rule 1: Runs segregation of duties checks. The action is not blocked and the violation is logged. Rule 2: Runs segregation of duties checks. The action is not blocked and the violation is logged.	Rule 1: Runs segregation of duties violation checks. The action is blocked. Rule 2: Runs segregation of duties violation checks. The action is blocked.
You use SOD Role Exclusion (36.3.27.8) to define a segregation of duties exclusion for a role. The exclusion rectifies an existing violation.	No segregation of duties checking.	Rule 1: Runs segregation of duties violation checks. The previous violation is fixed. Rule 2: Validates segregation of duties violation checks. The previous violation is fixed.	Not applicable.
You disable the Role is Excluded from SOD field in SOD Rule Exclusion (36.3.27.8). The role exclusion had caused a previous violation to be resolved, and is now reset.	No segregation of duties checking.	Rule 1: Runs segregation of duties violation checks. The action is not blocked and the violation is logged. Rule 2: Runs segregation of duties violation checks. The action is not blocked and the violation is logged.	Rule 1: Runs segregation of duties violation checks. The action is blocked. Rule 2: Runs segregation of duties violation checks. The action is blocked.
Segregation of duties is activated in SOD Configuration (36.3.27.14).	No segregation of duties checking.	Rule 1: Runs segregation of duties violation checks. The action is not blocked and the violation is logged. Rule 2: Runs segregation of duties checks. The action is not blocked and the violation is logged.	Rule 1: Runs segregation of duties violation checks. The action is blocked. Rule 2: Runs segregation of duties violation checks. The action is blocked.
Segregation of duties is disabled in SOD Configuration (36.3.27.14).	No segregation of duties checking.	Rule 1: Existing violations are fixed. Rule 2: Existing violations are fixed.	Not applicable.

Complete Prerequisite Activity

Before setting up segregation of duties, you must create user records in the system and provide basic identifying information. Use User Maintenance (36.3.1) to define users in your system. Users must be defined in the system before they can be assigned to a role. See “Set Up Users” on page 49.

You also can define user roles—but not role permissions or role membership—as a prerequisite activity. See “Define Roles” on page 66.

Disable the Superuser Role

The Superuser role is specially configured to provide assigned users with access to all resources in the system. Treat this role like a system administrator role, and only assign it to a few trusted users.

Before you activate segregation of duties, it is recommended that you use Role Modify (36.3.6.2) to disable the superuser role to prevent any further users from being added as role members.

It is also recommended that you select the Excluded from SOD field for the superuser role in SOD Role Exclusion (36.3.27.8). Excluding the superuser role from segregation of duties means that no segregation of duties violations will be raised for this role, which speeds up the activation of segregation of duties. See “Segregation of Duties Role Exclusions” on page 150.

Important If you attempt to activate segregation of duties and the Excluded from SOD field is cleared for the superuser role, a warning displays to indicate that the activation may not process correctly. You are then presented with the option to activate segregation of duties from the command line or to continue with the activation using the UI. If the Excluded from SOD field is not selected for the superuser role, it is recommended that you use the command line to activate segregation of duties. See “Activate Segregation of Duties from the Command Line” on page 140.

Activate Segregation of Duties

Use SOD Configuration (36.3.27.14) to activate segregation of duties rule checking on your system.

Fig. 8.7
SOD Configuration (36.3.27.14)

The screenshot shows the 'SOD Configuration' window. It has a title bar with 'SOD Configuration' and a close button. Below the title bar is a menu bar with 'Go To', 'Actions', 'Tools', 'Attach', 'Print', and 'Preview'. The main area is titled 'Attachments' and contains the following options:

- ☒ SOD active
- ☐ SOD block all rule violations
- Send SOD Notifications to User
- Send SOD Notifications to e-mail

SOD Active. Select the field to activate rule checking for segregation of duties.

If you activate segregation of duties, all validation rules are run to check for violations. You cannot continue implementing segregation of duties if role permission (Rule 1) violations exist on your system. You must deactivate segregation of duties, resolve the violations raised, and then reimplement segregation of duties.

When you first begin to implement segregation of duties, it is recommended that you deactivate segregation of duties rule checking, and only activate it again when you have defined all categories, the segregation of duties matrix, linked resources to segregation of duties categories, and defined roles. If you deactivate segregation of duties, the system does not check for role permission and role membership violations, and notification and logging are also disabled.

If you deactivate segregation of duties, all existing violations are deleted, and log entries are created for violations that were rectified.

SOD Block All Rule Violations. Select this field if the system must block any changes to role-based security that would allow users to access conflicting resources. The effect of selecting this field is that all indirect violations become blocked. Direct violations are always blocked, regardless of the setting of the SOD Block All Rule Violations field.

If this field is not selected, administrators are not blocked from providing users with access to functions with conflicting segregation of duties categories. However, any violations are still recorded in the log files.

Important Users are always blocked from performing actions in Role Permissions Maintain (36.3.6.5) that cause Rule 1 violations and are always blocked from performing actions in Role Membership Maintain (36.3.6.6) that cause Rule 2 violations.

If you select this field, the system prevents administrators from making changes to role-based security that violate role permission (Rule 1) and role membership (Rule 2) segregation of duties rules. If you activate blocking for rule violations, the violations log will always be empty because administrators are actively blocked from performing actions that violate segregation of duties rules.

When you enable this field, the system checks if violations exist, and displays an error if violations are found. The SOD Block All Rule Violations field cannot be enabled until these violations are fixed.

If you leave the field deselected, the system does not block an administrator from making changes to role-based security that violate role permission (Rule 1) and role membership (Rule 2) segregation of duties rules. The violations raised are written to the segregation of duties log. The default value is deselected.

Send SOD Notifications to User. In addition to on-screen notifications and the segregation of duties audit logs, the system can send notification of segregation of duties violations by e-mail. The system can send notifications to an external mail address or to the internal inbox of a user on the system.

If you want the system to send segregation of duties notification e-mails to a user, use the lookup to specify the user. The system uses the email address for the user configured in User Maintenance.

Send SOD Notifications to Email. If you want the system to send segregation of duties notification e-mails to an external e-mail address, specify the e-mail address in this field.

Activate Segregation of Duties from the Command Line

The following is an example of a shell script that you can use to activate segregation of duties from the command line.

Replace the bold text in brackets with values relevant to the environment on which you are running segregation of duties.

```
#####
#!/bin/sh
DLC=<PROGRESS_LOCATION>;export DLC
. <PROGRESS_LOCATION>bin/slib_env
PATH=$PATH:<PROGRESS_LOCATION>/bin;export PATH
PROMSGS=<PROGRESS_LOCATION>/promsgs;export PROMSGS
PROTERMCAPI=<PROGRESS_LOCATION>/protermcap;export PROTERMCAPI

<PROGRESS_LOCATION>/bin/_progres -pf <PATH_TO>/QADFinapp.pf -param "-action ActivateSOD
-PROPATH <FULL_PROPATH>" -b -p "<PATH_TO>/qadfin.pl<<program/applicationcontrol.r>>" >
<OUTPUT_FILE>.txt
#####
```

Maintain Segregation of Duties Categories

Use SOD Category activities (36.3.27.1) to create, modify, view, and delete segregation of duties categories. Add as many categories as required to accommodate your specific segregation of duties requirements.

Segregation of duties categories are used to group resources that share similar characteristics within an organization.

After defining your segregation of duties categories, use SOD Matrix Maintain (36.3.27.3) to specify which category codes are compatible with each other.

Fig. 8.8
SOD Category Create (36.3.27.1.1)

SOD Category Code. Enter a unique category name (maximum 20 characters).

SOD Category Description. Enter a description (maximum 40 characters) of the segregation of duties category.

When resources have been assigned to a segregation of duties category in SOD Category Membership Maintain (36.3.27.4), you can view the resources-to-category assignment in SOD Category Modify (36.3.27.1.2), SOD Category View (36.3.27.1.3), and SOD Category Delete (36.3.27.1.4) by selecting the View Linked Resources drop-down.

Fig. 8.9
SOD Category View, View Linked Resources Drop-Down

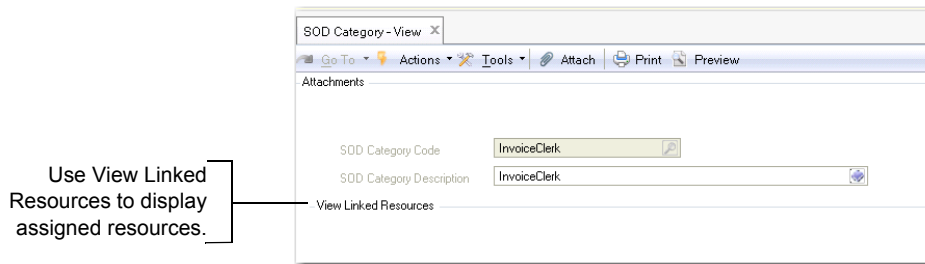
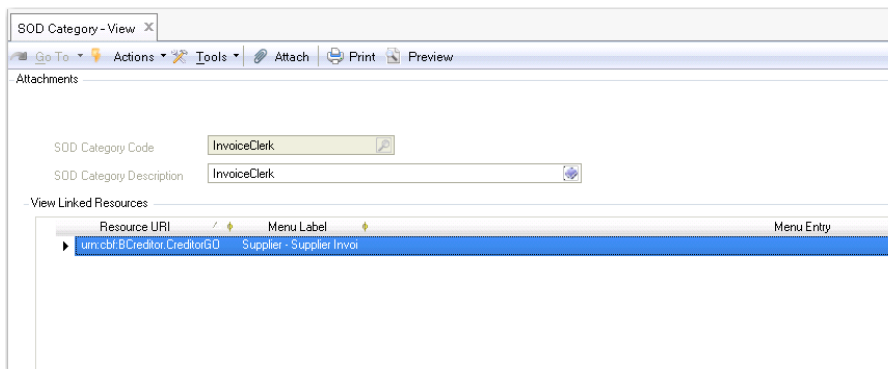


Fig. 8.10
SOD Category View, Linked Resources



Delete Categories

Use SOD Category Delete (36.3.27.1.4) to delete a segregation of duties category. You can only delete a segregation of duties category if it is not associated with a resource. If you try, a message displays.

When a segregation of duties category is deleted, the system recalculates the category compatibility matrix to remove the sets of pairs that contain the deleted category. The system also recalculates rule violations in the system, and logs the fixes.

After deleting a segregation of duties category, review the SOD Violations report (36.3.27.9) to verify that the resulting segregation of duties setup satisfies your internal controls requirements.

SOD Category Excel Integration

Use SOD Category Excel Integration (36.3.27.1.5) to export segregation of duties category records to or load records from an Excel spreadsheet.

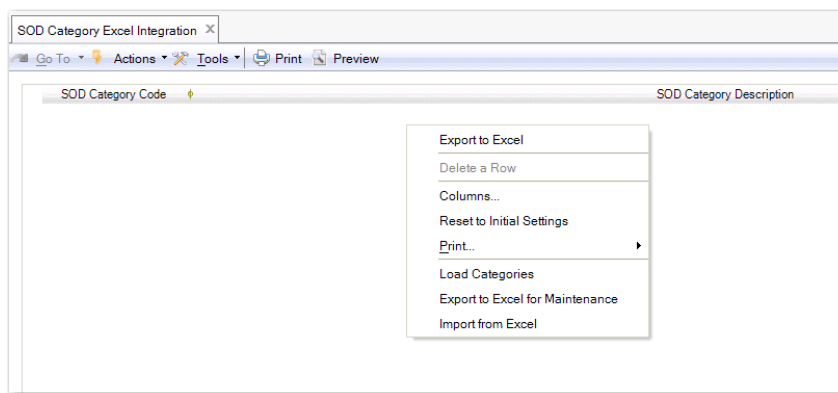
If you right-click and select Load Categories, the system shows all segregation of duties categories in the grid. You can then modify and save the segregation of duties category records.

If you right-click and select Export to Excel for Maintenance, the system downloads the loaded segregation of duties category records, and exports them to an Excel file for maintenance. You must specify the name and location of the exported Excel file. You can also select Export to Excel for Maintenance when the grid is empty. In this case, the system creates an Excel sheet with the relevant database field names headings for maintaining data.

If you right-click and select Import from Excel, you can select and load an Excel file containing segregation of duties category records. The Excel file must be in the correct format for importing and have the correct database field names as column headings.

In the SOD Category worksheet, you can add segregation of duties categories by inserting a new row and reloading the file. When modifying existing segregation of duties category data, you can change the category description only.

Fig. 8.11
SOD Category Excel Integration (36.3.27.1.5)



Assign Resources to Segregation of Duties Categories

Use SOD Category Membership Maintain (36.3.27.4) to maintain associations between an application resource—that is, an activity or a program represented by a menu item—and a segregation of duties category.

First, define segregation of duties categories in SOD Category Create (36.3.27.1.1) and specify the category compatibilities in SOD Matrix Maintain (36.3.27.3).

You select resources to assign to categories using a tree view similar to that in Role Permissions Maintain (36.3.6.5). The tree view shows the resources that are available on the menu and the hierarchical structure of the menu, and then shows the resources that are not available on the menu.

An application resource can be associated with only one category or with no category.

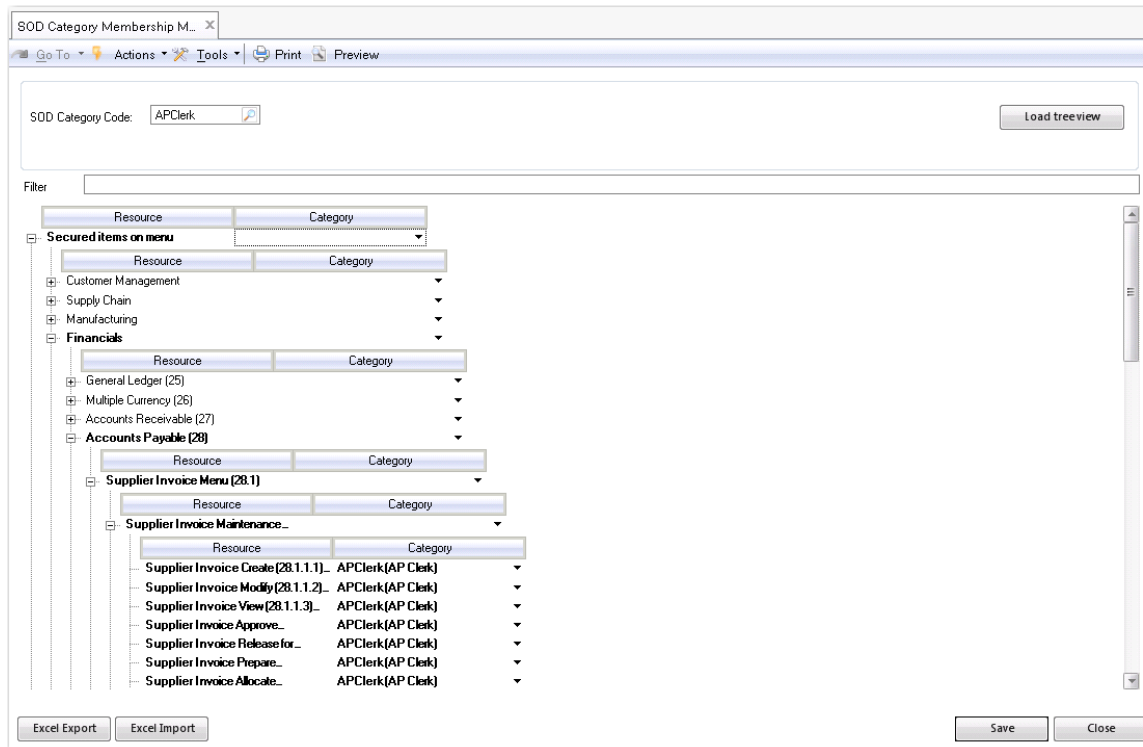
- If associated with a category, the resource is only compatible with other resources that are associated with resources with the same segregation of duties category, with resources that have a compatible segregation of duties category, and with all resources that are not linked to a segregation of duties category.
- If associated with no category, the resource is compatible with any other application resource, regardless of the segregation of duties category to which those resources are attached.

Example You associate Supplier Invoice Create with the segregation of duties category code SuppInvCr, and Supplier Payments Create with the segregation of duties category code SuppPayCr.

You select a category by typing the category code, or using the lookup. The Load Tree View button shows the resources assigned to the selected category in bold, providing an immediate visual indication of resources and category assignments.

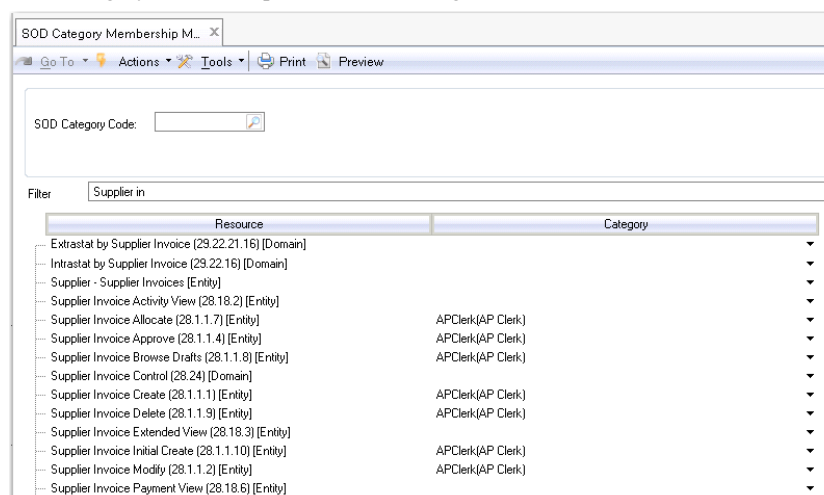
To assign a category to a menu resource, select the category from the drop-down list to the right of the resource name.

Fig. 8.12
SOD Category Membership Maintain (36.3.27.4)



To facilitate the assignment of resources, you can use the Filter field at the top of the screen to search for menu labels, menu item entry numbers, URNs, and segregation of duties categories.

Fig. 8.13
SOD Category Membership Maintain, Filtering



SOD Category Code (header). Specify a segregation of duties category and click the Load Tree View button to display the menu tree view with menu items assigned that segregation of duties category highlighted in bold.

Filter. Specify values to search for menu labels, menu item entry numbers, URNs, and segregation of duties categories.

Category (grid). Select a category from the drop-down on a grid row to assign that segregation of duties category to the resource on that row. A resource can only be associated with one category or no categories.

SOD Category Membership Excel Integration

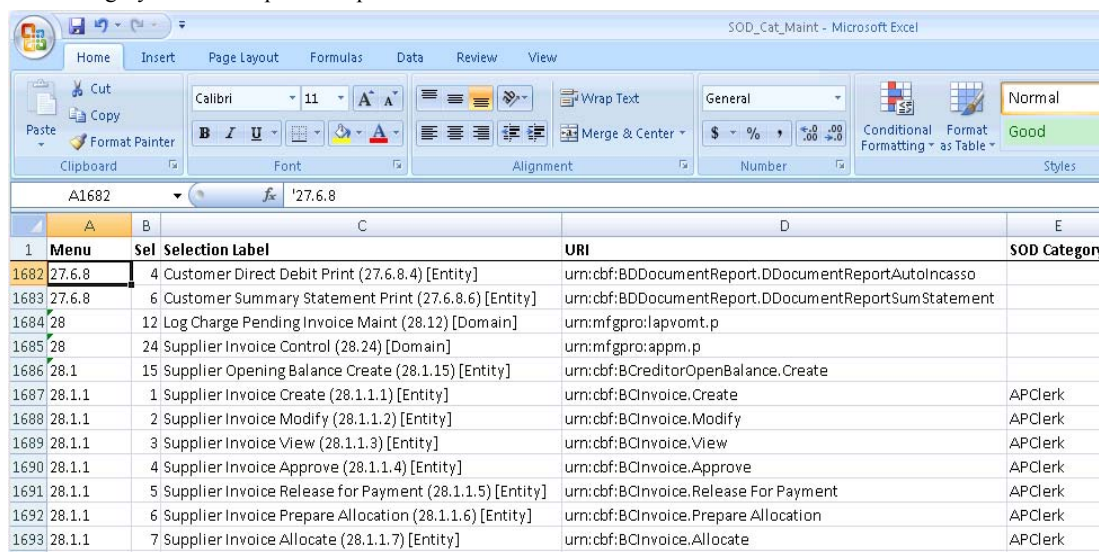
SOD Category Membership Maintain (36.3.27.4) contains options that let you export resource and segregation of duties category data to Excel, maintain the data offline, and re-import the data using Excel integration.

The Export to Excel option in SOD Category Membership Maintain (36.3.27.4) copies the matrix data to an Excel spreadsheet that you can save on your local drives.

In the exported spreadsheets, you can assign a category to a resource, change the category assigned to a resource, or clear the Category field to remove a resource and category assignment.

Use the Import from Excel option in SOD Category Membership Maintain (36.3.27.4) to re-import the modified Excel spreadsheet.

Fig. 8.14
SOD Category Membership Excel Spreadsheet



	A	B	C	D	E
1	Menu	Sel	Selection Label	URI	SOD Category
1682	27.6.8	4	Customer Direct Debit Print (27.6.8.4) [Entity]	urn:cbf:BDDocumentReport.DDocumentReportAutoIncasso	
1683	27.6.8	6	Customer Summary Statement Print (27.6.8.6) [Entity]	urn:cbf:BDDocumentReport.DDocumentReportSumStatement	
1684	28	12	Log Charge Pending Invoice Maint (28.12) [Domain]	urn:mfgpro:lapvont.p	
1685	28	24	Supplier Invoice Control (28.24) [Domain]	urn:mfgpro:apppm.p	
1686	28.1	15	Supplier Opening Balance Create (28.1.15) [Entity]	urn:cbf:BCreditorOpenBalance.Create	
1687	28.1.1	1	Supplier Invoice Create (28.1.1.1) [Entity]	urn:cbf:BCInvoice.Create	APClerk
1688	28.1.1	2	Supplier Invoice Modify (28.1.1.2) [Entity]	urn:cbf:BCInvoice.Modify	APClerk
1689	28.1.1	3	Supplier Invoice View (28.1.1.3) [Entity]	urn:cbf:BCInvoice.View	APClerk
1690	28.1.1	4	Supplier Invoice Approve (28.1.1.4) [Entity]	urn:cbf:BCInvoice.Approve	APClerk
1691	28.1.1	5	Supplier Invoice Release for Payment (28.1.1.5) [Entity]	urn:cbf:BCInvoice.Release For Payment	APClerk
1692	28.1.1	6	Supplier Invoice Prepare Allocation (28.1.1.6) [Entity]	urn:cbf:BCInvoice.Prepare Allocation	APClerk
1693	28.1.1	7	Supplier Invoice Allocate (28.1.1.7) [Entity]	urn:cbf:BCInvoice.Allocate	APClerk

Maintain the Segregation of Duties Matrix

Use SOD Matrix Maintain (36.3.27.3) to specify if a segregation of duties category is compatible with another segregation of duties category. The system stores the compatibility constraints you specify as a matrix, which is represented as a set of pairs of segregation of duties category codes. When you define categories, they are compatible with all other categories by default.

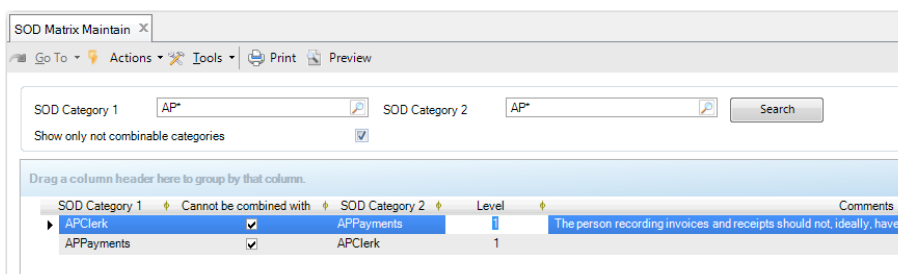
If you click the Search button in the header, all the segregation of duties category pairs currently defined in the system and their corresponding compatibilities are displayed.

You can then use the check box in the Cannot be Combined with column to indicate that two segregation of duties categories are mutually exclusive. If you indicate that two categories are mutually exclusive, you can assign a value from 1 to 5 to indicate the level of conflict between the categories.

You can refine the categories in the grid by entering values in the SOD Category 1 field, SOD Category 2 field, or both, and searching on those values. The system only populates the grid with segregation of duties categories that match your search criteria. The SOD Category 1 and SOD Category 2 fields support the wildcards “*” and “.”.

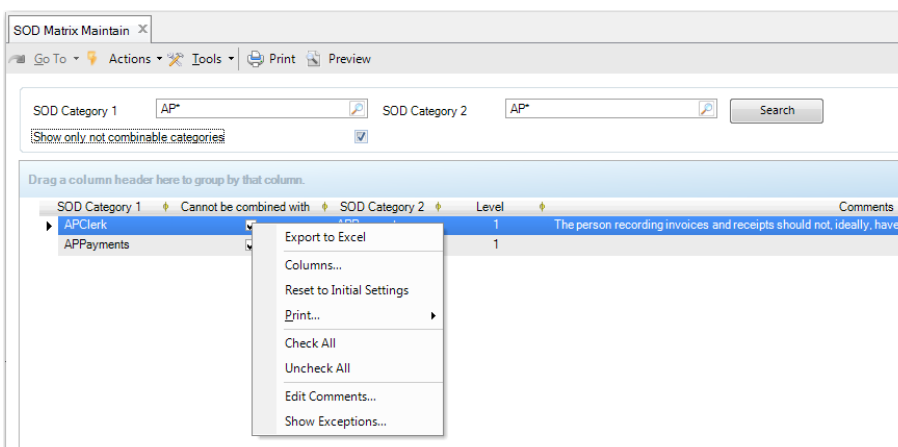
If you search on all categories or search using wildcards for two similarly-named categories, a segregation of duties category combination can appear twice in the grid; for example, one entry for InvoiceEntry-InvoiceAppr and another entry for InvoiceAppr-InvoiceEntry, based on the example in Figure 8.15. In this case, if you select the Cannot be Combined with field for one entry, the system selects the Cannot be Combined with field for the other entry automatically. The same applies for the Level and Comments fields. If you enter comments or a conflict level for a pair of categories, A and B, the same comments or conflict level also appear when the category pair is displayed in reverse order as B and A.

Fig. 8.15
Two Entries for the Same Two Mutually Exclusive Categories



A right-click context menu option is available for lines containing two mutually exclusive segregation of duties categories. The Show Exceptions option opens a browse with all known exceptions for this conflicting pair of categories.

Fig. 8.16
SOD Matrix Maintain, Context Menu



When you save new information, the system checks to see if segregation of duties policy violations have been introduced based on existing category assignments to application resources, resource assignments to roles, and user assignments to roles.

If the modified matrix introduces new segregation of duties violations, the system issues a warning and creates a log record for each violation. Use the SOD Violations Report (36.3.27.9) to identify any violations.

If the modified matrix fixes existing segregation of duties violations, the system logs this. This situation typically occurs if two incompatible categories are changed to be compatible.

If the SOD Block All Rule Violations field is selected in SOD Configuration (36.3.27.14), you are blocked from saving any matrix change that introduces segregation of duties violations.

Fig. 8.17
SOD Matrix Maintain (36.3.27.3)

SOD Category 1	Cannot be combined with	SOD Category 2	Level	Comments
APClerk	☒	APPayments	1	The person recording invoices and receipts should not, ideally, have access to create and process
APPayments	☒	APClerk	1	

SOD Category 1. Specify a segregation of duties category code for which you want to define compatibility.

SOD Category 2. Specify a segregation of duties category code for which you want to define compatibility.

Show only not combinable categories. Select the field to only display incompatible pairs for the segregation of duties category or categories you specified in the SOD Category 1 and SOD Category 2 search fields.

Grid

SOD Category 1. Enter a code that identifies a segregation of duties category defined in SOD Category Create (36.3.27.1.1).

SOD Category 2. Enter a code that identifies the segregation of duties category to be marked as compatible or incompatible with the first category code.

Cannot be Combined with. Select the field to indicate that the two category codes are mutually exclusive. If the field is not selected, this indicates that the category codes are compatible.

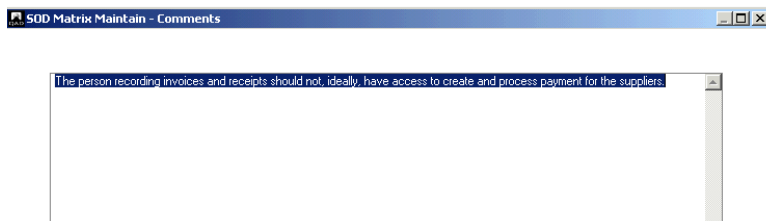
Level. Enter a value from 1 to 5 to associate a conflict level with the mutually exclusive category codes.

This field is only enabled if you select the Cannot Be Combined with field.

Comments. Enter text to explain why the two categories are mutually exclusive. Because the comments are typically more than just one line, you can right-click and open a dialog box in which you can enter your comments. The Comments field in the grid only shows the first part of the comment.

Note If you deselect the Cannot be Combined with field, the comments you recorded for the two categories that were previously mutually exclusive are cleared the next time you save.

Fig. 8.18
SOD Matrix Maintain, Comments Dialog



SOD Matrix Excel Integration

SOD Matrix Maintain (36.3.27.3) contains options that let you export segregation of duties matrix data to Excel, maintain the data offline, and re-import the data using Excel integration.

The Export to Excel option in SOD Matrix Maintain (36.3.27.3) copies the matrix data to an Excel spreadsheet that you can save on your local drive. The Excel spreadsheet only contains the data that you have displayed in the grid. Therefore, if you have refined the SOD Matrix Maintain (36.3.27.3) search criteria to only display a limited number of categories in the grid, only this information is exported to Excel.

Fig. 8.19
SOD Matrix Maintain Excel Spreadsheet

	A	B	C	D	E	F
1	SOD Category 1	INV*				
2	SOD Category 2	INV*				
3						
4	SOD Category 1	Cannot be combined with	SOD Category 2	Level	Comments	
5	InvoiceEntry	Yes	InvoiceAppr	1		
6	InvoiceAppr	Yes	InvoiceEntry	1		
7						
8						
9						

A segregation of duties category combination can appear twice in the grid, for example, one entry for InvoiceEntry-InvoiceAppr and another entry for InvoiceAppr-InvoiceEntry. In this case, both rows are exported to Excel.

You can import your modified segregation of duties matrix spreadsheet using the Import from Excel option in SOD Matrix Maintain (36.3.27.3).

If there are two entries in the segregation of duties matrix spreadsheet for the same segregation of duties category combination (for example, A-B and B-A), you must modify both rows if you want to update the segregation of duties matrix for these categories. If you modify one row, for example, to add comments or deselect the compatibility indicator, but do not make an identical modification to the other row, the system displays a screen indicating that conflicts exist.

Fig. 8.20
SOD Matrix Maintain, Conflicts

Conflicts are found. Please select the correct lines to use.

#	Selected	SOD Category 1	Cannot be combined with	SOD Category 2	Level	Description
1	☒	APClerk	☒	APPayments	1	The person
1	☐	APPayments	☒	APClerk	2	

For every conflict found, you must indicate which of the conflicting pairs you want to import by selecting the Selected field. In the example shown in Figure 8.20, the Cannot be Combined with indicator has a different value for the otherwise identical pairs for categories APClerk/APPayments and APPayments/APClerk. In this example, the user selects the field to indicate that the first row is the correct one, and this value is imported.

Define Role Permissions

Use Role Permissions Maintain (36.3.6.5) to associate application resources with a role. Application resources must be associated with a role to be available to a system user. See “Define Role Permissions” on page 67 for details on this program.

If a role currently has no resources associated with it, the role can be associated with any resource. If a role has existing associations, it can only be associated with a resource that has a segregation of duties category that is compatible with the existing categories in the role’s segregation of duties category set.

If you try to associate an application resource with a role that has an incompatible segregation of duties category, the system displays an error message and the association is not saved. Use SOD Matrix Maintain (36.3.27.3) to maintain the compatibility of segregation of duties categories. See “Maintain the Segregation of Duties Matrix” on page 144.

If a user has been assigned one or more roles, the user can be assigned to the role only if each of roles is compatible with the current role, or if there is a policy exception that exempts any incompatible pair of roles.

If you try to assign a user to a role that is incompatible with one or more of the roles already assigned to the user, when you attempt to update the database the system displays an error and does not assign the role.

When a user is restricted from using an application resource, the user cannot access a resource by typing its name.

Define Role Membership

Use Role Membership Maintain (36.3.6.6) to associate users and user roles. The associations you create between users and roles in this step are now constrained by the defined segregation of duties policy.

For more information on defining role membership, see “Define Role Membership” on page 70.

Maintain Segregation of Duties Policy Exceptions

Use SOD Policy Exception Create (36.3.27.2.1) to maintain segregation of duties policy exceptions. Defining a policy exception gives a specified user access to a pair of resources that are not compatible under segregation of duties policy.

Segregation of duties policy exceptions are sometimes necessary to accommodate situations—for example, unforeseen absences in the workplace—that require a user to perform tasks outside of their usual responsibilities.

Note Although the system does not constrain the number of segregation of duties policy exceptions that can be defined, if it becomes apparent that many policy exceptions are required, this may indicate that your segregation of duties security model should be reviewed. Policy exceptions are intended to accommodate exceptional circumstances, rather than systemic inadequacies in a segregation of duties policy framework.

A policy exception is associated with a domain and, optionally, an entity within a domain. If an entity is not specified, the policy exception applies to all entities within the specified domain.

Policies are checked any time a change is made that impacts segregation of duties; for example, when a user is assigned to a role, when you link resources to categories, when you change role permissions, or when you change role membership.

When you add a user to a role, the system validates that the roles the user already belongs to are compatible with the new role assigned. If they are not compatible, the system searches for a policy exception for this user. If no exception is found, an error is generated and the user cannot be added to the role.

Example The MediCare company wants to implement segregation of duties. Normally, for good internal control, the user who implements and maintains system security should be different than the user who implements segregation of duties. However, MediCare is a small company with a small IT department and one system administrator. Therefore, the system administrator is assigned both the roles for Security Maintenance and SOD Maintenance.

Fig. 8.21
SOD Policy Exception Create (36.3.27.2.1)

Domain	Entity	SOD category 1 code	SOD category 2 code	Description
Domain1	SecurAdmin	SODAdmin		We need to allow this exception for our system administrator.

Exception Code. Enter a policy exception code.

Exception Description. Enter a description of the policy exception.

This field describes the business reason underlying this policy exception and may be required for auditing purposes. You can include information about compensating controls (that is, management controls that are outside the system) that your organization uses to mitigate risks arising from the exception.

User Login. Enter a user ID to identify the user to whom this policy exception applies.

Fig. 8.22
SOD Policy Exception Create, Category Details

Allowed Exceptions				
Domain	Entity	SOD category 1 code	SOD category 2 code	Description
Domain1		SecurAdmin	SODAdmin	We need to allow this exception for our system administrator.

Domain. Specify the domain in which this policy exception applies.

Entity. Specify the entity in which this policy exception applies for the specified user. If no entity is entered, the policy exception applies to all entities within the domain.

SOD Category Code 1. Specify the first category in the pair for which this exception applies.

SOD Category Code 2. Specify the second category in the pair for which this exception applies. If you have specified the first category and that category is defined as being incompatible with only one other segregation of duties category, the second segregation of duties category defaults automatically.

Description. Enter a detailed description of why the policy exception is required for the segregation of duties categories. This field is optional.

After you have defined segregation of duties policy exceptions, use Role Membership Maintain (36.3.6.6) to associate users with the user roles that have been defined as part of your segregation of duties policy exceptions. See “Define Role Membership” on page 70.

Delete Policy Exceptions

To delete a segregation of duties policy exception, use SOD Policy Exception Delete (36.3.27.2.4).

Defining a segregation of duties policy exception prevents violations from being raised when a user is assigned to incompatible categories in role exceptions. If you delete a policy exception and SOD blocking is enabled, the user is prevented from performing tasks relating to segregation of duties categories that are incompatible with other segregation of duties categories for roles to which the user is assigned.

If you delete a policy exception and SOD blocking is disabled, the user can perform tasks relating to incompatible segregation of duties categories, but segregation of duties violations are logged.

Segregation of Duties Role Exclusions

Use SOD Role Exclusion (36.3.27.8) to specify that a particular role is exempt from segregation of duties rule checks and blocking. This option is particularly useful for roles applied to technical superuser accounts used to query the database and perform actions when external systems integrate with QAD Financials.

Segregation of duties role exclusion is the highest level of segregation of duties policy exception and should be used carefully.

Fig. 8.23
SOD Role Exclusion (36.3.27.8)

Role Name. Specify the role that is exempt from segregation of duties. The role must already be defined in Role Create (36.3.6.1).

Role Description. This field displays a description of the role.

Active. Indicates whether the role is active or inactive.

Exclude from SOD. Select the field to exclude the role from segregation of duties violation checks and blocking, if enabled.

If the Exclude from SOD field is selected and avoids existing Rule 1 and Rule 2 violations, you cannot clear this field if the SOD Block All Rule Violations field is selected in SOD Configuration (36.3.27.14).

If the SOD Block All Rule Violations field is cleared in SOD Configuration (36.3.27.14), the system logs the relevant violations if you clear the Exclude from SOD field.

Import and Export Segregation of Duties Data

SOD Import/Export (36.3.27.15) lets you create and load default data for segregation of duties categories, matrices, resource assignments, and roles using a single Excel spreadsheet. The function lets you check for role permission (Rule 1) and role membership (Rule 2) violations before saving the data to the database.

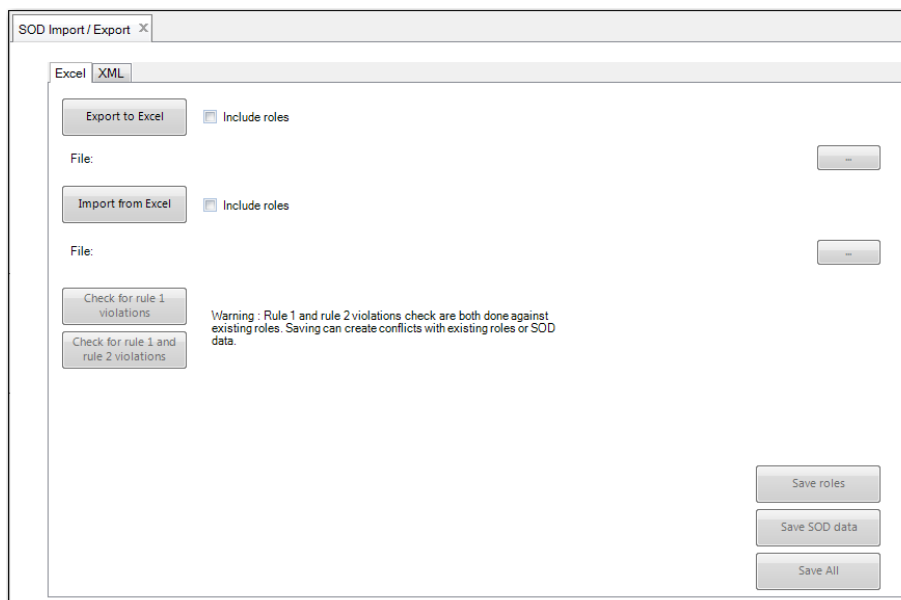
You can export segregation of duties data to an XML file to create default XML data that can be loaded during the deployment process. You can also import data from an XML file, which facilitates the loading of default SOD data. If you reload the default SOD data after you have modified SOD categories or the SOD matrix, the reloaded SOD default data overwrites the modifications and restores the SOD categories and matrix settings defined in the default data.

Important The default SOD data provided by QAD is based on best practices, and has not been validated by an external audit company.

The Excel spreadsheet you export using SOD Import/Export (36.3.27.15) contains four worksheets:

- SOD Category
- SOD Matrix
- Resource
- Role

Fig. 8.24
SOD Import/Export (36.3.27.15)



SOD Category Worksheet

In the SOD Category worksheet, you can add segregation of duties categories by inserting a new row and reloading the file. When modifying existing segregation of duties category data, you can change the category description only. You cannot change the segregation of duties category code because the system would interpret a changed category as a new category when you load the data.

Fig. 8.25
SOD Category Worksheet

	A	B	C	D	E	F	G	H	I	J	K	L
1	SOD Category Code	SOD Category Description										
2	BudgetCreate	Budget Creation										
3	ConsolAdmin	Consolidation Admin										
4	CtInvApp	Customer Invoice Approval										
5	CtInvClerk	Customer Invoice Clerk										
6	CustDataAdmin	Customer Data Admin										
7	POCreate	PO Creation										
8	PORceipt	PO Receipt										
9	SecurAdmin	Security Admin										
10	SODAdmin	SOD Admin										
11	SplnvApp	Supplier Invoice Approval										
12	SplnvClerk	Supplier Invoice Clerk										
13	SysAdmin	SystemAdministrator										

SOD Matrix Worksheet

In the SOD Matrix worksheet, you can add new matrix lines or delete existing lines by setting the value in the Cannot be Combined with column to No. See “SOD Matrix Excel Integration” on page 147 for more information on SOD Matrix Excel integration.

Fig. 8.26
SOD Matrix Worksheet

A	B	C	D	E
1 SOD Category 1	Cannot be combined with	SOD Category 2	Level	Comments
2 CtlInvApp	No	SplInvApp		
3 CtlInvClerk	No	SplInvClerk		
4 CtlInvClerk	Yes	CtlInvApp	1	
5 POCreate	Yes	POReceipt		
6 BudgetCreate	No	CustDataAdmin		
7 SplInvClerk	Yes	SplInvApp		
8 SysAdmin	Yes	SecurAdmin		
9 ConsolAdmin	No	BudgetCreate		
10 SecurAdmin	Yes	SODAdmin		

Resource Worksheet

In the Resource spreadsheet, you can only add or remove segregation of duties categories. See “SOD Category Membership Excel Integration” on page 144.

Fig. 8.27
Resource Worksheet

A	B	C	D	E	F
1 Menu	Sel	Selection Label	URI	SOD Category	
1084 19.2	2	Procedure Browse (19.2.2) [Domain]	urn:mfgpro:qcbro03.p		
1085 19.2	3	Procedure Report (19.2.3) [Domain]	urn:mfgpro:qctsr.p		
1086 19.25	1	Update Blank Master Specification (19.25.1) [Domain]	urn:mfgpro:utmpnbr.p		
1087 19.3	1	Sampling Pattern Maintenance (19.3.1) [Domain]	urn:mfgpro:qcsprmt.p		
1088 19.3	2	Sampling Pattern Browse (19.3.2) [Domain]	urn:mfgpro:qcbro01.p		
1089 19.3	3	Sampling Pattern Report (19.3.3) [Domain]	urn:mfgpro:qcsprp.p		
1090 19.3	13	Sample by Expire Days Inquiry (19.3.13) [Domain]	urn:mfgpro:qclsiq.p		
1091 19.3	14	Sample by Lot Interval Inquiry (19.3.14) [Domain]	urn:mfgpro:qclsiq02.p		
1092 2	9	Op Address List Type Maint (2.9) [Domain]	urn:mfgpro:adlsmt.p		
1093 2	10	Op Address List Type Browse (2.10) [Domain]	urn:mfgpro:adbr008.p		
1094 2	12	Company Address Maintenance (2.12) [Domain]	urn:mfgpro:admgmt06.p		
1095 2.1	1	Customer Data Maintenance (2.1.1) [Domain]	urn:mfgpro:adcsmt.p		
1096 2.1	2	Customer Browse (2.1.2) [Domain]	urn:mfgpro:cmbr101.p		
1097 2.1	4	Customer Data Report (2.1.4) [Domain]	urn:mfgpro:adcsrp01.p		
1098 2.1	5	Customer Labels Print (2.1.5) [Domain]	urn:mfgpro:adcsrp02.p		
1099 2.1	6	Customer Data View (2.1.6) [Domain]	urn:mfgpro:adcsvw.p		
1100 2.1	12	Master Comment Maintenance (2.1.12) [Domain]	urn:mfgpro:gpcmmt.p		
1101 2.1	14	Customer Ship-To Inquiry (2.1.14) [Domain]	urn:mfgpro:adstiq.p		
1102 2.1	15	Customer Ship-To Address Report (2.1.15) [Domain]	urn:mfgpro:adstip.p		
1103 2.1	18	Salesperson Assignment Report (2.1.18) [Domain]	urn:mfgpro:adcsrp03.p		
1104 2.1	24	Dock Control (2.1.24) [Domain]	urn:mfgpro:adcsrp.p		
1105 2.1.9	1	Reserved Location Maintenance (2.1.9.1) [Domain]	urn:mfgpro:adrlmt.p		
1106 2.1.9	2	Reserved Location Browse (2.1.9.2) [Domain]	urn:mfgpro:adrlbr.p		

Role Worksheet

In the Role spreadsheet, you can indicate whether roles are active or inactive, and indicate which roles are excluded from segregation of duties. See “Segregation of Duties Role Exclusions” on page 150.

Fig. 8.28
Role Worksheet

	A	B	C	D	E	F	G
1	Role Name	Role Description	Active	Exclude from SOD			
2	SuperUser	SuperUser Role	TRUE	TRUE			
3	EmployeeNotify	Create employee	TRUE	FALSE			
4	SupplierNotify	Create of supplier	TRUE	FALSE			
5	CustomerNotify	Create of customer	TRUE	FALSE			
6	EndUserNotify	Create of enduser	TRUE	FALSE			
7	RptDesigner	Report Designer	TRUE	FALSE			
8	rptAdmin	Report Administrator	TRUE	FALSE			
9	CROBA1	CRreate Open Balance	TRUE	FALSE			
10	CROBA2	CRreate Open BALance	TRUE	FALSE			
11	rptAdmin2	Report Administrator	TRUE	FALSE			
12	rptDsgn2	Report Developer	TRUE	FALSE			
13	JERole1	role for journal entry	TRUE	FALSE			
14	JERole2	role for journal entry	TRUE	FALSE			
15	RMRole	role for receiver match	TRUE	FALSE			
16	FMRole	role for fin matching	TRUE	FALSE			
17	ConsRole	role for consolidation	TRUE	FALSE			
18	SanRole	Sanity Role	TRUE	FALSE			

Export to Excel

The Export to Excel option in SOD Import/Export (36.3.27.15) creates an Excel file in the format required for reloading data to the system.

When you click the Export to Excel button, the system asks if you want to include data already in the system. If you answer Yes, the Excel sheet created contains all segregation of duties data already in the system.

If you select the Include Roles check box, the system displays a dialog that lets you specify the roles for which to export data.

Fig. 8.29
SOD Import/Export, Role Selection

Export	Role Name	Description
☒	SanRole	Sanity Role
☒	initiate	Initiator
☒	approver	approver
☒	role1	role1
☒	role2	role2
☒	Reporting	mnt. variants+sch
☒	QXtendRole	QXtend Role
☒	LCI	LCI
☒	ReceiverMatching	Role 28.x

SOD Import/Export (36.3.27.15) displays the name and path of the exported or imported Excel file below the Export to Excel and Import from Excel buttons.

Fig. 8.30
Name and Path of Exported Excel File

SOD Import / Export

Excel XML

Export to Excel ☒ Include roles

File: C:\Users\ymg\Desktop\ExportedSODandRoles.xlsx

Import from Excel ☐ Include roles

File:

Check for rule 1 violations

Check for rule 1 and rule 2 violations

Warning : Rule 1 and rule 2 violations check are both done against existing roles. Saving can create conflicts with existing roles or SOD data.

Save roles

Save SOD data

Save All

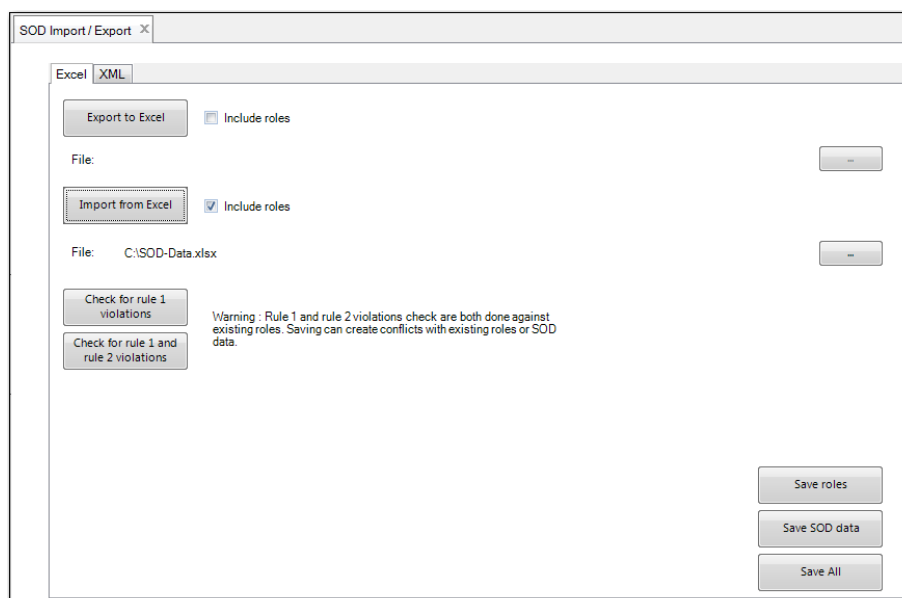
Import from Excel

Use the Import from Excel option to load an Excel spreadsheet of segregation of duties default data.

If you select the Include Roles check box, the system imports also role data if the spreadsheet has a roles worksheet and data. When you import segregation of duties and role data, you have three options: save the role data only, save the segregation of duties data only, or save both types of data.

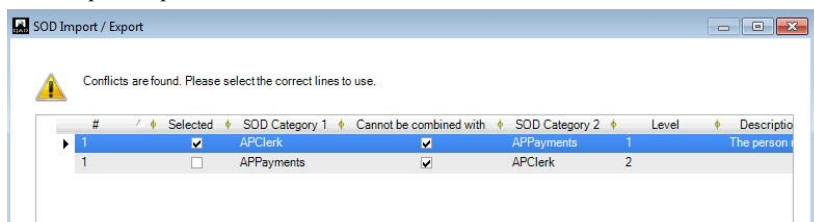
When you load a spreadsheet, the Check for Violations buttons are activated. Click the buttons to determine if the loaded data generates segregation of duties violations.

Fig. 8.31
Check for Violations Buttons Activated



As with the Excel Integration function in SOD Matrix Maintain (36.3.27.3), when importing from Excel, if there are two entries in the SOD Matrix spreadsheet for the same segregation of duties category combination (for example A-B and B-A), you must modify both rows if you want to update the segregation of duties matrix for these categories. If you modify one row, for example, to add comments or deselect the compatibility indicator, but do not make an identical modification to the other row, the system displays a screen indicating that conflicts exist.

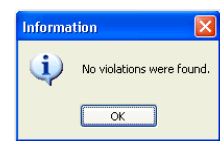
Fig. 8.32
SOD Import/Export, Conflicts



For every conflict found, you must indicate which of the conflicting pairs you want to import by selecting the Selected field.

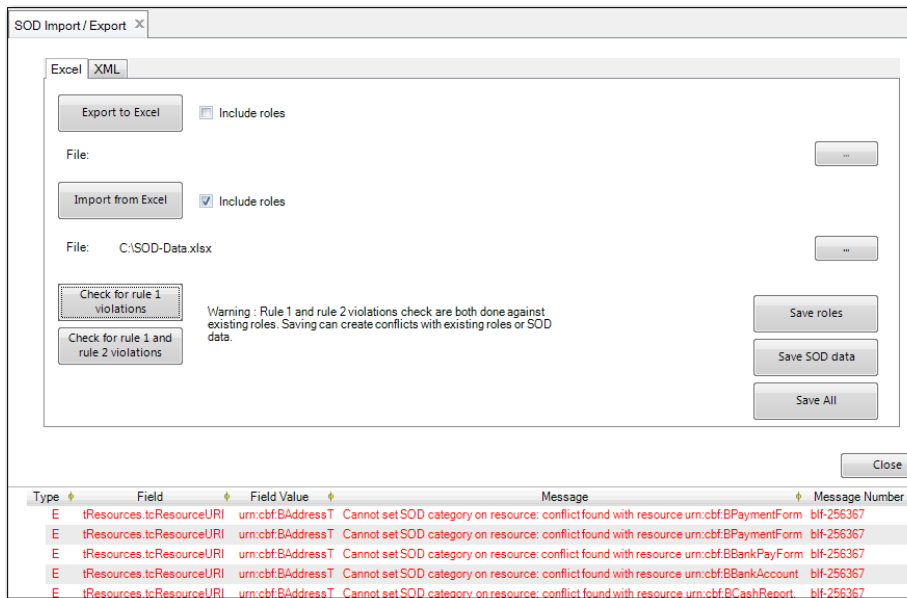
When you load the data, if no violations are found when you select a Check for Violations button, the system displays a dialog indicating this.

Fig. 8.33
No Violations Found



If you click a Check for Violations button and the loaded data contains segregation of duties violations, the violation errors are displayed at the end of the screen.

Fig. 8.34
Violation Errors



The Check for Violations buttons become disabled when no new data is loaded after performing the segregation of duties violation rule checks.

Export to XML

The Export to XML option exports segregation of duties data to an XML file. This XML data can then be used during deployment.

The following data is exported:

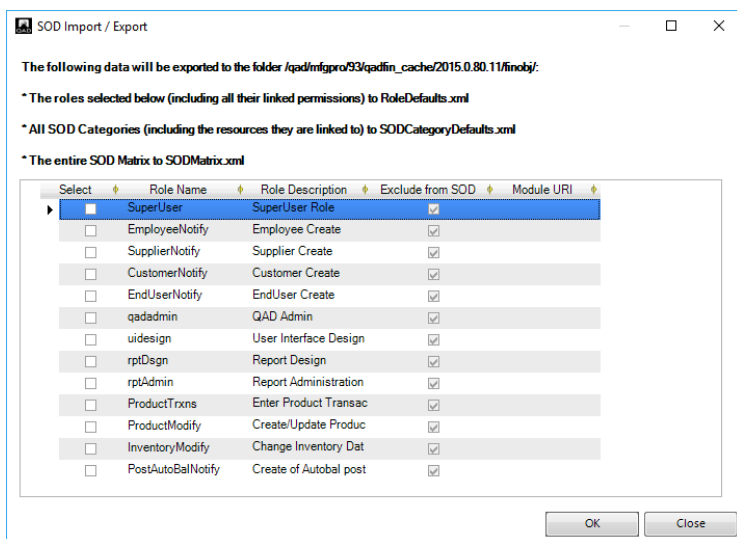
- Roles
- Role permissions
- Segregation of duties categories
- Segregation of duties matrix
- Segregation of duties resource linking

The segregation of duties data is exported to the following three files:

- RoleDefaults.xml
- SODCategoryDefaults.xml
- SODMatrix.xml

In the XML Export dialog, select the fields in the column on the left to indicate the roles for which you want to export XML data.

Fig. 8.35
XML Export Dialog



Import from XML

The Import from XML option can be used to import default segregation of duties data from an XML file.

The function loads three files from a default location on your system. The files are stored in the same location as factory defaults and report variants.

As with Export from XML, you can import roles, permissions, and segregation of duties categories.

The segregation of duties data is imported from the following three files:

- RoleDefaults.xml
- SODCategoryDefaults.xml
- SODMatrix.xml

The loaded data is merged with the existing data, if any, and all segregation of duties rules are checked. If blocking violations occur, the load fails.

Report and View Logs and Violations

View Log History

The SOD Log Viewer (36.3.27.6) lets you view logs of changes that impacted the segregation of duties rules over time, such as rule violations and actions that rectified rule violations.

The browse grid shows:

- User Login
- Role Name
- SOD Category 1

- SOD Category 2
- Resource 1 URI
- Resource 2 URI
- Whether an action caused Rule 1 (role permissions) or Rule 2 (role membership) to be violated or fixed
- Fix date – time
- Conflict date – time
- Login ID of the user who caused or fixed the violation.

Fig. 8.36
SOD Log Viewer (36.3.27.6)

The screenshot shows the 'SOD Violations Log Browse for...' window. It includes a toolbar with 'Actions', 'Print', 'Add to Favorites', 'Chart', 'Chart Designer', 'Refresh', and 'Stored Searches'. Below the toolbar is a search section with filters for SOD Category 1, SOD Category 2, Entity, Time Stamp of Creation, Domain, and Modifying User, each with a dropdown menu set to 'equals' and a search button. The main table displays a list of violations with columns for SOD Category 1, SOD Category 2, Entity, Time Stamp of Creation, Domain, Modifying User, and Resource 1 URI. The table shows 17714 records, with the first 10 displayed.

SOD Category 1	SOD Category 2	Entity	Time Stamp of Creation	Domain	Modifying User	Resource 1 URI
Category-6	Category-2	1000	06/10/2010 13:11:17.310+01:00	Domain1	kdm	urn:cbf:BCInvoice.Replace
Category-6	Category-1	1000	06/10/2010 13:11:17.308+01:00	Domain1	kdm	urn:cbf:BCInvoice.Replace
Category-6	Category-2	1000	06/10/2010 13:11:17.306+01:00	Domain1	kdm	urn:cbf:BCInvoice.Release For Payment
Category-6	Category-1	1000	06/10/2010 13:11:17.304+01:00	Domain1	kdm	urn:cbf:BCInvoice.Release For Payment
Category-6	Category-2	1000	06/10/2010 13:11:17.301+01:00	Domain1	kdm	urn:cbf:BCInvoice.Prepare Allocation
Category-6	Category-1	1000	06/10/2010 13:11:17.299+01:00	Domain1	kdm	urn:cbf:BCInvoice.Prepare Allocation
Category-6	Category-2	1000	06/10/2010 13:11:17.297+01:00	Domain1	kdm	urn:cbf:BCInvoice.Approve
Category-6	Category-1	1000	06/10/2010 13:11:17.295+01:00	Domain1	kdm	urn:cbf:BCInvoice.Approve
Category-6	Category-2	1000	06/10/2010 13:11:17.294+01:00	Domain1	kdm	urn:cbf:BCInvoice.Allocate
Category-6	Category-2	1000	06/10/2010 13:11:17.292+01:00	Domain1	kdm	urn:cbf:BCInvoice.Allocate
Category-6	Category-2	1000	06/10/2010 13:11:17.291+01:00	Domain1	kdm	urn:cbf:BCInvoice.Allocate
Category-6	Category-2	1000	06/10/2010 13:11:17.290+01:00	Domain1	kdm	urn:cbf:BCInvoice.Allocate
Category-6	Category-2	1000	06/10/2010 13:11:17.288+01:00	Domain1	kdm	urn:cbf:BCInvoice.Allocate
Category-6	Category-1	1000	06/10/2010 13:11:17.286+01:00	Domain1	kdm	urn:cbf:BCInvoice.Allocate
Category-6	Category-1	1000	06/10/2010 13:11:17.285+01:00	Domain1	kdm	urn:cbf:BCInvoice.Allocate

Report on Current Segregation of Duties Conflicts

Use the SOD Violations report (36.3.27.9) to determine whether there are compliance violations for role permissions, role membership, or both in the system.

The report has the following filter fields:

- Entity
- Domain
- Role
- User
- Include rule 1 (Yes/No)
- Include rule 2 (Yes/No)
- Exclusion Level
- Include Resource Details (Yes/No)

Figure 8.37 illustrates the selection criteria for the SOD Violations report (36.3.27.9).

Fig. 8.37
SOD Violation Report, Selection Criteria

The screenshot shows the 'SOD Violations Report - Viewer' window. It has a menu bar with 'Filter' and 'Viewer' tabs. Below the menu bar is a toolbar with buttons for 'New Filter', 'OPEN_FILE_OR_DOC', 'Save', 'Save As', 'Delete', 'Settings', 'Layout', 'Document', 'Run', and 'Schedule'. The main area is titled 'Search Conditions' and contains a table of criteria:

Field	Operator	Value	+	-
Include resource data	equals	No	+	-
Include rule 1	equals	Yes	+	-
Include rule 2	equals	Yes	+	-
Entity	contains		+	-
Domain	contains		+	-
Exclusion Level	contains		+	-
Role	contains		+	-
User	contains		+	-

A report option lets you indicate whether the report should display details or not. If you specify the details option, the report also provides a list of the resources linked to the conflicting categories.

The SOD Violation report (36.3.27.9) contains two sections: Rule 1 Violations and Rule 2 Violations.

The Rule 1 Violations section displays the following data on role permission violations:

- Role name
- SOD category 1 code and description
 - Resources of category 1 used in the role
- SOD category 2 code
 - Resources of category 2 used in the role

The Rule 2 Violations section displays the following data on role membership violations:

- User name
- Scope (domain name or entity name or blank)
- Role 1 name
- SOD category 1 code
 - Resources of category 1 used in the role
- Role 2 name
- SOD category 2 code
 - Resources of category 2 used in the role

Category codes are displayed with their description. Resources are displayed with their corresponding menu entry and label.

Fig. 8.38
SOD Violations Report (36.3.27.9)



SOD Violations

Date: 6/11/2010

Time: 03:20:52

PaymentsClerk	Payments Clerk	Category-3	Category-3-description
		Category-4	Category-4-description
		Menu Number	Resource Label

View Role Permissions Violations

Use SOD Violations Rule 1 View (36.3.27.10) to display details of role permission violations.

Fig. 8.39
SOD Violations Rule 1 View (36.3.27.10)

SOD Rule 1 Violations Browse...

Actions

Print

Add to Favorites

Chart

Chart Designer

Refresh

Stored Searches

Search (3)

Role Name

equals

SOD Category 1 Cod

equals

SOD Category 2 Cod

equals

Search

Clear All

Viewing 1 - 18 of 18

Records per page: All

Creation Date	Creation Time	Created By	Role Name	SOD category 1 code	SOD category 2 code
6/10/2010	12:05:26	kdm	KDMWorkflow	Category-5	Category-6
6/10/2010	12:05:26	kdm	SIA-Test	Category-5	Category-6
6/10/2010	12:05:27	kdm	JERole1	Category-7	Category-8
6/10/2010	12:05:29	kdm	JERole2	Category-7	Category-8
6/10/2010	12:05:29	kdm	RMRole	Category-1	Category-5
6/10/2010	12:05:29	kdm	RMRole	Category-1	Category-6
6/10/2010	12:05:29	kdm	RMRole	Category-5	Category-6
6/10/2010	12:05:30	kdm	FMRole	Category-1	Category-5

Use SOD Violations Rule 2 View (36.3.27.11) to display details of role membership violations.

Comments? Go to goo.gl/MfwKHm

QAD

Fig. 8.40
SOD Violations Rule 2 View (36.3.27.11)

Entity Code	Domain	Creation Date	Creation Time	Created By	Role 1 Name	Role 2 Name	SOD category 1 code	SOD category 2 code
NGH-CONS	Domain1	6/10/2010	12:05:38	kdm	KDMworkflow	SIA-Test	Category-5	Category-6
NGH-CONS	Domain1	6/10/2010	12:05:38	kdm	bazrole	SIA-Test	Category-5	Category-6
NGH-CONS	Domain1	6/10/2010	12:05:38	kdm	bazrole2	SIA-Test	Category-5	Category-6
NGH-NGH	Domain3	6/10/2010	12:05:38	kdm	KDMworkflow	SIA-Test	Category-5	Category-6
NGH-NGH	Domain3	6/10/2010	12:05:38	kdm	bazrole	SIA-Test	Category-5	Category-6
NGH-NGH	Domain3	6/10/2010	12:05:38	kdm	bazrole2	SIA-Test	Category-5	Category-6
domain10	Domain10	6/10/2010	12:05:38	kdm	KDMworkflow	SIA-Test	Category-5	Category-6

Archive Log Record Files

Use SOD Log Archive (36.3.27.7) to archive log records when an online history of segregation of duties violations is no longer needed.

The archive facility lets you archive the segregation of duties logs up to a certain date. The log is written to an XML or a CSV file, and the segregation of duties log data up to the date you specify is removed from the SOD Log Viewer (36.3.27.6).

When implementing security in your system, you should restrict access to this program.

Fig. 8.41
SOD Log Archive (36.3.27.7)

Filename on Server. Specify the name that you want to assign to the segregation of duties log archive file.

Archive Up To Date. Specify the date up to which you want to archive segregation of duties logs. Segregation of duties log data up to that date is removed from the SOD Log Viewer (36.3.27.6).

E-signatures

This section discusses how to set up and use e-signatures functionality in your system.

Overview 164

Explains the purpose of the e-signatures features, lists eligible programs, describes the planning steps when implementing e-signatures, illustrates the e-signatures workflow, and explains QAD-specified categories, tables, and fields.

Set Up E-Signature Functionality 169

Explains the steps necessary to set up records that control when e-signatures are recorded.

E-Signature Categories 170

Describes e-signature categories and the category considerations, tables, fields, and filters.

E-Signature Profiles 176

Describes e-signature profiles and lists the steps required to set up and use e-signature profiles.

Record E-Signatures 185

Describes how e-signatures are processed through the system with details on transaction scoping and product change control.

E-Mail Notifications 187

Explains how and when the system generates and sends e-mails to system users and lists the different types of notifications.

Reporting 188

Lists the areas through which reports and inquiries are available and gives details about each type.

Archive and Restore Records 193

Describes how to use E-Signature Archive/Delete to archive e-signature records to files and delete records when they are obsolete.

Overview

Regulatory guidance often requires records to be signed by an author, approver, tester, or other accountable individual, particularly in areas with critical processes that rely on tight quality control such as the pharmaceuticals industry.

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 e-signatures can be used to support automated processing.

The e-signatures features of the Enhanced Controls menu support this requirement. You can configure your system to require users of some 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.

Note Any valid user who has access to a function that records signatures can sign records. Use Role Permissions Maintain (36.3.6.5) to assign access to signature-controlled functions based on user roles. See “Define Role Permissions” on page 67.

These features are intended as part of an overall approach—also incorporating capabilities offered by system security—to meeting the user accountability requirements of customers with regulated environments.

E-signature Enabled Programs

E-signature functionality is limited to a subset of programs, tables, and fields that are defined in QAD-provided default signature profiles. See “Tables and Fields” on page 173. Table 9.1 lists the programs that currently can have e-signatures enabled.

Table 9.1
Programs Included in Default Profiles

Module	Menu	Program
Product Change Control (PCC)	1.9.2.8	PCR/PCO Detail Inquiry
	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
	1.9.9.1	Print PCR/PCO
Regulatory Attributes	1.22.1	Lot Master Maintenance
	1.22.2	Lot Master Inquiry
	1.22.24	Regulatory Attributes Control

Module	Menu	Program
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
	3.6.5	Inventory Detail Report
	3.21.1	Transactions Detail Inquiry
	3.24	Inventory Control
Process	4.8.16	Inventory Detail Maintenance
Shop Floor Control	16.20.1	Labor Feedback by Work Order
	16.20.2	Labor Feedback by Employee
	16.20.3	Labor Feedback by Work Center
	16.20.4	Non-Productive Labor Feedback
	16.20.5	Operation Complete Transaction
	16.20.6	Operation Move Transaction
	16.20.13.9	Operation Transaction Detail Inq
	16.20.13.14	Operations By Work Order Report
Item Attributes and Quality Control	16.20.13.15	Operations By Employee Report
	19.3.1	Quality Order Results Maint
	Collection	Maintain Quality Order
	Collection	Maintain Quality Order for Purchasing
	Collection	Maintain Quality Order for SO Line
	Collection	Maintain Quality Order for Production
	Collection	Edit Closed Quality Order
	19.3.12.1	Quality Test Record Maint
	NA	Quality Order Test Records
	Collection	Maintain CUM Order Op Test Record
	Collection	Maintain Work Order Op Test Record
	Collection	Edit Closed Quality Test Record
	NA	Edit Closed CUM Order Op Test Record
	Collection	Edit Closed Work Order Op Test Record
	1.15.21.1	Lot Attribute Order Maint
	Collection	Maintain Lot Attribute Order
	Collection	Maintain Lot Attribute Order for Purchasing
	Collection	Maintain Lot Attribute Order SO Line
	Collection	Maintain Lot Attribute Order for Production
	Collection	Edit Closed Lot Attribute Order
	19.1.1	Test Specification Maint
	Collection	Maintain Test Specification
	19.8.1	Certificate of Analysis Print
Quality Management	19.26.11	QM Quality Order Results Entry
	19.26.12	QM Quality Order Results Report

Module	Menu	Program
Master Data Reports	19.26.13	QM Test Results Maintenance
	19.26.15	QM Test Results Report
	19.26.20	QM Certificate of Analysis Print
	36.17.6	Control Tables Report

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 192.

The e-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 e-signature functionality. Adding new categories requires custom development.

Programs for E-Signature Setup and Reporting

Table 9.2 shows the programs available for setting up and reporting on e-signature functions.

Table 9.2
E-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
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
36.12.14.13	E-Sig Initial Data Load	esinild.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

E-Signature Planning Steps

Before e-signature processing can begin, the prerequisite planning steps must be completed.

The first activity in setting up e-signature functions is to plan the extent to which you need to require signatures.

- Determine the types of data that need to be signed based on the regulatory requirements for your specific industry or environment.
- Determine how QAD Enterprise Applications fits into your overall business processes, as well as which specific e-signatures support those processes.
- Complete data mapping requirements for records and available signatures.
- Determine security requirements for signed records; for example, assign appropriate role-based security to prevent users who should not sign records from accessing the programs that require signatures.

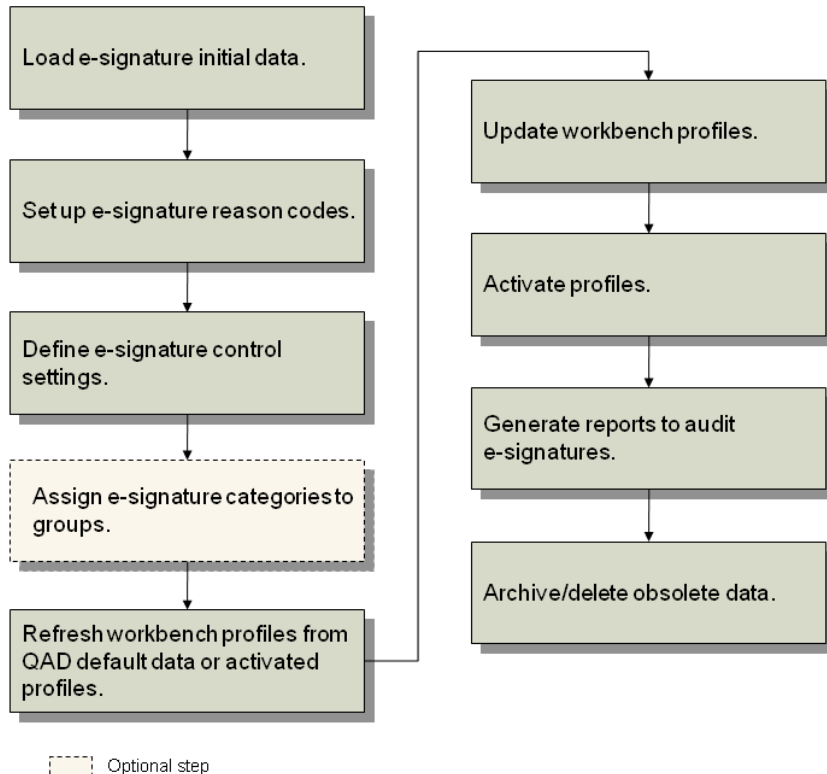
Note E-signatures should be part of a detailed security plan to meet your overall business requirements.

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 the system 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.

E-Signature Workflow

The following e-signature workflow, in Figure 9.1 can be used to set up e-signature functions in your environment.

Fig. 9.1
E-signatures Workflow



- 1 **Load e-signature initial data.** Use E-Sig Initial Data Load (36.12.14.13) to load the initial data (QAD-provided default profiles) into the system. See “Load E-signature Initial Data” on page 169.
- 2 **Set up e-signature reason codes.** E-signature reason codes are a critical component because they explain the meaning of each signature. Reason codes describe whether the person applying the signature was approving, inspecting, reviewing, or so on. Be sure to plan and implement reason codes that make sense in your specific regulatory environment. All reason codes used by e-signatures must have an “ESIG” reason type. See “Set Up E-signature Reason Codes” on page 169.
- 3 **Define e-signature control settings.** When setting up e-signature functionality, define the security control settings in Security Control (36.3.24) to determine how sign-in security is defined in terms of password structure and use rules. See “Define Security Control Settings” on page 170.
- 4 **Optionally, assign e-signature categories to groups.** Optionally, define e-signature groups to simplify the setup process. To avoid repetitive data entry for individual category profiles, create signature groups in E-Signature Group Maintenance (36.12.14.1). See “E-Signature Categories” on page 170.
- 5 **Refresh workbench profiles from QAD default data or activated profiles.** See “Refresh Signature Profiles” on page 178.

- 6 **Update workbench profiles.** When initially setting up e-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. See “Refresh Profile Frame” on page 179
- 7 **Activate 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 e-signature functions to begin on a future date; signature settings are not in effect 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 “Activate E-signature Profiles” on page 184.
- 8 **Generate reports to audit e-signatures.** Use E-Signature Events Report (36.12.4) and E-Signature History Report (36.12.5) to view information that applies to e-signatures. Use E-Signature Failure Report (36.12.7) as part of your security program to identify potential unauthorized access attempts. See “E-signature Records for Quality Control” on page 189.
- 9 **Archive/delete obsolete data.** Use E-Signature Archive/Delete (36.12.14.22) to archive e-signature records to a file and optionally delete the records from the system when they are no longer needed online. See “Archive and Restore Records” on page 193

Set Up E-Signature Functionality

When setting up e-signature functionality, the following tasks must be completed:

- Load E-signature Initial Data
- Set Up E-signature Reason Codes
- Define Security Control Settings

Load E-signature Initial Data

The initial data, QAD-provided default profiles, must be loaded into the system first. Use E-Sig Initial Data Load (36.12.14.13) to load the data.

Enter the directory of the files and all the default profiles in that directory will be loaded into the system. These files are located on the server side under *installdir*/config/electronic-signature, where *installdir* is the root application installation directory.

Set Up E-signature Reason Codes

The signature reason code is a critical element of the e-signature. In regulatory environments, the signature record typically must include the meaning of the signature. The system uses reason codes to provide the meaning.

Each time the system prompts for an e-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. See “Record E-Signatures” on page 185.

Use Reason Codes Maintenance (36.2.17) to define signature reason codes that are appropriate to your environment.

Important All reason codes used by e-signatures must be associated with the QAD-provided ESIG reason type. Reasons of any other type cannot be entered in the signature prompt frame.

Define Security Control Settings

To prevent any unauthorized individuals from applying e-signatures using another user's ID, e-signatures uses the same validation logic used in the sign-in process. See Chapter 2, "Security Overview," on page 13 for information on setting up and using sign-in security.

When setting up e-signature functionality, define the security control settings in Security Control (36.3.24) to see how sign-in security is defined in terms of password structure and use rules.

Fig. 9.2
Security Control (36.3.24)

These fields control access for e-signature processing.

Two fields directly control how the system manages unsuccessful e-signature attempts:

- **Maximum Access Failures** indicates how many consecutive unsuccessful signature attempts cause the user's session to terminate, disable the account, and inform the administrator role of a potential unauthorized access attempt.
- **Administrator Role** is the name of the role—defined in Role Create (36.3.6.1)—assigned to the system users who are notified by e-mail when a session is terminated because of excessive unsuccessful signature attempts. The system also sends e-mail to users who are assigned this role when a signature profile is activated. See "E-Mail Notifications" on page 187.

E-Signature Categories

A category is a QAD-provided definition of a set of system 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 database 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 16.20) 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 QM 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 175.

Table 9.3 lists the e-signature categories, as well as the default menu programs associated with them. If you do not want a particular program to generate e-signatures, you can clear its selection in the workbench profile. See “Apply Profile to Menu Programs” on page 182.

Table 9.3
QAD-Defined Categories

Code	Name	Description	Available Menu Programs
0001	InvCtrl	Inventory Control	Inventory Control (3.24) Control Tables Report (36.17.6)
0002	QMRes	QM Quality Results	Labor Feedback by Work Order (16.20.1) Operations by Work Order Report (16.20.13.14) Operations by Employee Report (16.20.13.15) Operation Transaction Detail Inq (16.20.13.9) Labor Feedback by Employee (16.20.2) Labor Feedback by Work Center (16.20.3) Operation Move Transaction (16.20.6) QM Test Results Maintenance (19.26.13) QM Test Results Report (19.26.15)
0003	OpHist	Operation History	Labor Feedback by Work Order (16.20.1) Operations by Work Order Report (16.20.13.14) Operations by Employee Report (16.20.13.15) Operation Transaction Detail Inq (16.20.13.9) Labor Feedback by Employee (16.20.2) Labor Feedback by Work Center (16.20.3) Non-Productive Labor Feedback (16.20.4) Operation Complete Transaction (16.20.5) Operation Move Transaction (16.20.6)
0004	ComCtrl	Regulatory Attributes Control	Regulatory Attributes Control (1.22.24) Control Tables Report (36.17.6)
0005	LotMstr	Lot Master	Lot Master Maintenance (1.22.1) Lot Master Inquiry (1.22.2)
0006	InvDet	Inventory Details	Inventory Detail Maintenance (3.1.1) Detail Maintenance by Item/Lot (3.1.2) Inventory Detail Report (3.6.5) Inventory Detail Maintenance (4.8.16)

Code	Name	Description	Available Menu Programs
0007	InvTran	Transaction History	Inventory Detail Maintenance (3.1.1) Detail Maintenance by Item/Lot (3.1.2) Transactions Detail Inquiry (3.21.1) Transfer–Single Item (3.4.1) Transfer with Lot/Serial Change (3.4.3) Batchload Transfer with Lot/Serial Change (3.4.4) QM Quality Order Results Entry (19.26.11)
0008	QMOrd	QM Quality Order	QM Quality Order Results Entry (19.26.11) QM Quality Order Results Report (19.26.12) QM Certificate of Analysis Print (19.26.20)
0009	PCOInc	PCO Incorporation	Incorporation Selection (1.9.7.4) Incorporation (1.9.7.5) Implementation (1.9.7.13) PCR/PCO Detail Inquiry (1.9.2.8) Print PCR/PCO (1.9.9.1)
0010	PCOAppr	PCO Approval	PCR/PCO Detail Inquiry (1.9.2.8) PCR/PCO Approval (1.9.6.1) Detail Approval Maintenance (1.9.6.13) Print PCR/PCO (1.9.9.1)
0011	QualOrd	Quality Order	Quality Order Results Maint (19.3.1) Maintain Quality Order Maintain Quality Order for Purchasing Maintain Quality Order for SO Line Maintain Quality Order for Purchasing Edit Closed Quality Order
0012	QualTest	Quality Test Record	Quality Test Record Maint (19.3.12.1) Maintain CUM Order Op Test Record Maintain Work Order Op Test Record Edit Closed Quality Order Test Record Edit Closed CUM Order Op Test Record Edit Closed Work Order Op Test Record
0013	LotAtOrd	Lot Attribute Order	Lot Attribute Order Result Maint (1.15.21.1) Maintain Lot Attribute Order Maintain Lot Attribute Order for Purchasing Maintain Lot Attribute Order for SO Line Maintain Lot Attribute Order for Production Edit Closed Lot Attribute Order
0014	TestSpec	Test Specification	Test Specifications Maintenance (19.1.1) Maintain Test Specification
0015	COA	Certificate of Analysis	Certificate of Analysis Print (19.8.1)

Note Some categories are also associated with reports and inquiries that can include e-signature data. See “Functional Reports and Inquiries” on page 192 for information.

Use E-Sig Category Master Report (36.12.14.11) to view information about the QAD-defined categories.

Category Considerations

Category 0007 Considerations

Current signature data for category 0007, Transaction History, is never shown as part of the latest e-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 “Record E-Signatures” on page 185.

Note You can still view the final data being signed in the final signature data frame for this category.

Category 0006 Id_det Records

Some companies choose to implement temporary locations by setting Permanent to No in Location Maintenance (1.1.18). This setting has consequences for how audit records are created and how e-signatures occur. This section outlines the effects of auditing and signing temporary location detail records (Id_det).

Inventory Detail Maintenance (3.1.1) and Detail Maintenance by Item/Lot (3.1.2) create the following transactions for non-permanent locations:

- ISS-CHL transaction is created in tr_hist that sets the QOH to zero and deletes the Id_det record.
- RCT-CHL transaction is created in tr_hist that receives the quantity on hand (QOH) for the new inventory detail record that is created for the temporary location.

This standard behavior may lead to some confusion in understanding the audit history because three audit records are created:

- One to delete the temporary Id_det record
- One to create it with all new values
- One to update the QOH

The delete event is for a different Id_det record than the create and modify.

When e-signatures are enabled, only one signature for these three events is captured. The signature is associated with the last event. This may appear to be misleading in the E-Signature History Report (36.12.5).

If you typically use temporary locations, you should consider this before enabling e-signatures on this type of record.

Tables and Fields

The category profile includes a list of tables and fields that define the data to be signed in the corresponding signature-enabled programs. See “Update Signature Profiles” on page 179.

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 16.20). View default profiles using E-Sig Workbench Profile Report (36.12.14.6) with Display Default Profiles set to Yes.

Fig. 9.3
Example of Workbench Profile Table/Field Structure

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_cmnt - Comment Data
	No Field		>> cmt_domain - Domain
Field in child-level table			

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.

You can specify top-table field values to identify 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. See “E-signature Reports” on page 189.

Filters

Depending on the specific requirements of your environment, you may not need to record e-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 e-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 QM Quality Results	✓	✓	✓		✓
0003 Operation History	✓	✓	✓		✓
0004 Regulatory Attributes Control	✓				
0005 Lot Master	✓		✓		
0006 Inventory Detail	✓	✓	✓	✓	
0007 Transaction History	✓	✓	✓	✓	
0008 QM Quality Order	✓	✓	✓	✓	
0009 PCO Implementation	✓				
0010 PCO Approval	✓				
0011 Quality Order	✓	✓	✓	✓	
0012 Quality Test Record	✓	✓	✓		✓
0013 Lot Attribute Order	✓	✓	✓	✓	
0014 Test Specification	✓				
0015 Certificate of Analysis	✓	✓	✓		

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 183.

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 e-signature. In this scenario, updating a record associated with site 1000, loc3 would not trigger a prompt for an e-signature.

In the same example, defined as an *exclusion* filter, e-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.

A profile can have either inclusion or exclusion filters, but not both.

E-Signature Profiles

Overview

The e-signature system maintains signature information based on a signature profile that is associated with a specific category of data. Profiles are identified by the corresponding QAD-defined category codes. The category profile specifies:

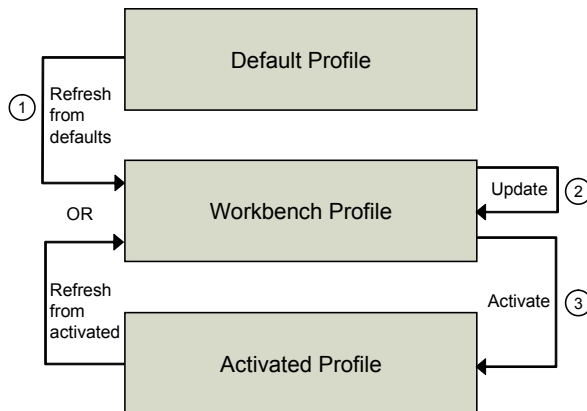
- Whether e-signatures are required
- In which programs
- Which fields are signed
- Characteristics of how signatures are displayed and recorded
- Filter definitions

The life cycle of a profile consists of three phases:

- **The QAD-provided default profile.** Based on QAD-provided category data, this is loaded using E-Sig Initial Data Load (36.12.14.13) 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 “Refresh Signature Profiles” on page 178.
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. Because the workbench profile has no effect on current system activities, you can continue to update it while the active version controls e-signature processing. See “Update Signature Profiles” on page 179.
- **The activated profile.** This is the profile used by the system to control e-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. See “Activate E-signature Profiles” on page 184.

Figure 9.4 summarizes the relationships between the three category profile types.

Fig. 9.4
Profile Flow



Setting up and using e-signature profiles include these steps:

- Create e-signature groups.
- Refresh workbench profiles.
- Update workbench profiles.
- Activate profiles.

Define E-Signature Profiles

Each category is associated with one or more signature-eligible 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 e-signature functions use to manage the information retention and reporting process. This information affects e-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 e-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 e-signature requirements apply to all records or only those containing specified values.

The system maintains three sets of profiles: the QAD-supplied default profiles, the profiles you edit in the workbench, and the activated profiles. See “Tables and Fields” on page 173. 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.

Create Signature Groups

Use E-Signature Group Maintenance (36.12.14.1) to group all the categories you plan to control using e-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.

Specify a group name, up to eight characters. An e-signature group cannot have the same name as a category code.

Next, provide a brief description and choose Next 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.

Refresh Signature Profiles

When initially setting up e-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.

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. If Value is blank, the system prompts you to confirm.

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 e-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.

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 e-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.

Note This field is available only when Source Profile is Activated.

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.

E-Signature On. Indicate whether to enable e-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.

Update 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 e-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

To disable e-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. See “Activate E-signature Profiles” on page 184.

Use E-Signature Workbench Profile Report (36.12.14.6) to display the information updated in this program.

Note Some special considerations apply when you are setting up profiles that involve category 0007, Transaction History. See page 173 for information.

Specifying Control Settings

Figure 9.5 illustrates the first frame of E-Signature Workbench Profile Maintenance.

Fig. 9.5

E-Signature Workbench Profile Maintenance (36.12.14.5)

Enter a QAD-defined category code and choose Next. The system displays several fields you can use to control e-signature processing.

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, QM 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 e-signature could contain many records of this type—so the mph_hist identification is not unique. However, all mph_hist records from the e-signature instance are related to a single wr_route record, which serves as a unique identifier for the signed data. See “Tables and Fields” on page 173.

E-Signature On. Indicate whether the system should apply the e-signature functions for the category defined in this profile when it is activated.

No: E-signatures do not apply to this category. Use this option to turn e-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, e-signature functions stop on the new profile’s begin date.

Yes: Once this profile is activated, e-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.

Display Latest E-Sig. Indicate whether the system displays the latest e-signature when programs controlled by this profile are executed. See “Record E-Signatures” on page 185.

When you refresh from QAD-provided default data, the value 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. This feature does not apply to all signature-enabled programs.

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 e-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 leave their computer 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 e-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.

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 e-signature data. When this field is Yes, a 64-character updateable Remarks field displays in the signature frame. Remarks are included in the e-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 e-signatures. See “Filters” on page 175.

None: Filters are not used. The Filters and Filter Criteria frames do not display.

Inclusion: Only data meeting the specified filter criteria requires e-signatures.

Exclusion: All data except those meeting the specified filter criteria require e-signatures.

Note A profile can have either inclusion or exclusion filters, but not both.

When you refresh from QAD-provided default data, the value is None.

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 (16.20.1) Labor Feedback by Employee (16.20.2) Labor Feedback by Work Center (16.20.3) Operation Move Transaction (16.20.6)	1. Operation History (0003) 2. QM Quality Results (0002)
QM Quality Order Results Entry (19.26.11)	1. Transaction History (0007) 2. QM Quality Order (0008)

Apply Profile to Menu Programs

When you initially set up e-signature functions by refreshing profiles based on QAD-provided data, each category is associated with one or more 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. See “Functional Reports and Inquiries” on page 192. 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.

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 173.

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.

These settings determine whether e-signature processing occurs for data associated with specified values. See “Filters” on page 175.

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.

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 e-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.

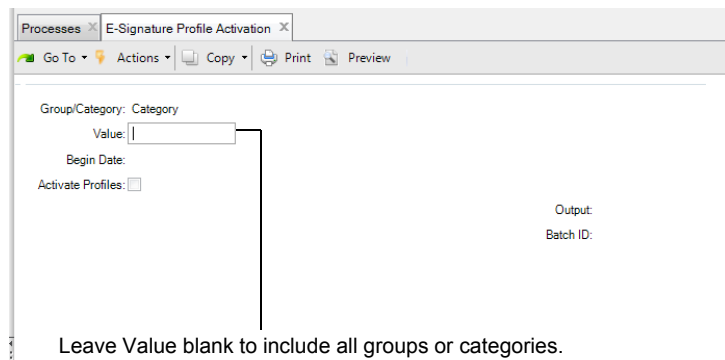
Important Since the system does not validate this value, you should be careful when you set up filters. For example, if you are setting up an inclusion filter to require e-signatures only for a single site and accidentally enter an invalid site code, the program will never prompt for a signature.

Activate E-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 e-signature functions to begin on a future date; signature settings are not in effect immediately after a profile is activated.

Fig. 9.6

E-Signature Profile Activation (36.12.14.8)



Group/Category: Category

Value:

Begin Date:

Activate Profiles: ☐

Output:

Batch ID:

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 173.

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.

When a profile is activated, the system automatically sends an e-mail message to system users who are assigned to the administrator role in Security Control (36.3.24). See “E-Mail Notifications” on page 187.

Record E-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 e-signatures based on rules defined in the active profile.

When Display Latest E-Sig is Yes in the active profile, before displaying data defined by the category, the system displays the signature that was recorded most recently for that data.

Note Latest signature data for category 0007, Transaction History, is not included in the display for programs associated with that category. See page 173.

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. Event ID is a system-assigned identifier for a specific e-signature.

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. See “Tables and Fields” on page 173.

Note If the 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 e-signature.

Note The points at which a program saves updates to the database may change when e-signatures are enabled. See “Transaction Scoping” on page 186.

The prompt screen includes the signature frame, as well as a details frame showing the data being signed.

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. See “Prompt for Preview E-Sig” on page 181. 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.

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, password, and a valid reason code defined for reason type ESIG. Note that the User ID field must be the same as your system sign-in ID. Depending on the Prompt for Remarks field in the active profile, you may also be able to enter a remark related to the signature.

If 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 sign 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, disable your user ID, and inform the system administrator of a potential unauthorized access attempt. See “Define Security Control Settings” on page 170.

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 signed 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.

Transaction Scoping

So that the system can apply e-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. See “Apply Profile to Menu Programs” on page 182.

For example, before e-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 Next, 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 Next through all the frames.

However, all frames are now part of one transaction block—allowing the system to apply the same e-signature to all updates made in the program. If you update the first frame, choose Next, and choose End in the second frame, the changes you made in the first frame are not saved to the database. You must choose Next through all the frames to save any changes you make in the program.

Product Change Control

If you use e-signatures with the Product Change Control (PCC) menu, 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 e-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 e-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 e-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 system users who are assigned the administrator role in Security Control (36.3.24) in the following situations:

- One or more signature profiles are activated.
- A user's consecutive number of failed e-signature attempts exceeds the Maximum Access Failures value in Security Control.

For more information see “Define Security Control Settings” on page 170.

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 (2.1.12).

The e-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 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 a QAD process. If you have any questions about this E-mail, contact the QAD 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 role identified in Security Control. 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 a QAD process. If you have any questions about this E-mail, contact the QAD 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 system users who are assigned the administrator role 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 disabled 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 role identified in Security Control.

User ID deactivated for exceeding max e-sig failures allowed: XXX

This email was automatically generated from a QAD process. If you have any questions about this email, contact the QAD system administrator. Do not reply to this email.

Reporting

Reports and inquiries related to e-signatures are available in three areas:

- Setup
- E-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 e-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.

E-signature Records for Quality Control

E-signature records that are created for quality orders, test records, test specifications, certificates of analysis, and lot attribute orders can be viewed from the collections that are used to maintain those documents. To view the e-signature record, navigate to the correct collection, select the document, and then select the E-Signature Events tab.

This functionality simplifies the process of finding and displaying the e-signature records for a document, as would be requested by an internal user, customer, or certification auditor.

The E-Signature Events tab contains a browse that displays all the electronic records for the selected document. Select a specific row on the browse to see an alternate view with the details of the electronic record.

E-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 e-signature history.
- Monitor sign-in history records for failed e-signature attempts.

View 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. 9.7
E-Signature Events Report (36.12.4)

View Signature History

Use E-Signature History Report (36.12.5) to select database records and view historical e-signature data associated with them. For example, you can report on the two latest signature events associated with a specified work order.

Fig. 9.8
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. Category is a required field. Use the following fields to control other characteristics of the report:

Max Events. Specify the maximum number of e-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 e-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 e-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.

Press Next 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.

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. See “Top Tables” on page 174.

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 Next. 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.

All fields are preselected if Auto-Select All is Yes in the first frame. Select or deselect fields as needed. Then press Next 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 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.

Monitor Failed Signature Attempts

As part of an overall security program, you can generate a report showing unsuccessful signature attempts, based on user sign-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 disabled because of excessive failed signature attempts.

When failed sign-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 named `esig_fail_YYYYMMDD.hst` where `YYYYMMDD` is the date you run E-Sig Failure Archive/Delete. If this function runs multiple times a day, the data will be appended to the same file for the given day.

Functional Reports and Inquiries

Some reports and inquiries associated with signature-enabled menu programs let you include e-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:

- E-Signature On is set to Yes. See page 179.
- The menu program has Apply selected. See page 182.

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 E-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 Browse	3.2	0006
Inventory Detail by Site Browse	3.3	0006
Inventory Detail Report	3.6.5	0006
Inventory Detail by Location	3.6.6	0006
Inventory Detail Report	3.6.5	0006
Transactions Detail Inquiry	3.21.1	0007
Operation Transaction Detail Inquiry	16.20.13.9	0003
Operations by Work Order Report	16.20.13.14	0003
Operations By Employee Report	18.4.14	0003
QM Quality Order Results Report	19.26.12	0008
QM Certificate of Analysis Print	19.26.20	0008
Control Tables 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, e-signature data is not included regardless of this setting. Change the output device to view that data. This limitation does not apply to reports.

Archive and Restore Records

Use E-Signature Archive/Delete (36.12.14.22) to archive e-signature records to a file and optionally delete the 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.

Select records by entering the last e-signature creation date you want the system to consider. The system selects all records up to that date that have not previously been archived. The archive data file has the format of `esig_data_YYYYMMDD.hst`. If this archive function is executed multiple times a day, the data will be appended to the same file.

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.

In E-Signature Restore (36.12.14.23), enter the date range of the records and the data file name to restore e-signature records.

Auditing

This section discusses how to set up the auditing functionality in your system.

Overview 196

Defines auditing and explains how the Auditing module works.

Plan Auditing 197

Describes what to consider before performing an audit.

Set Up Auditing 198

Describes the requirements for configuring auditing for databases, importing policies, enabling auditing for specific areas, and generating audit reports.

Archive Database 204

Describes how to set up archive databases, connections, report on them, and customize archive/load scripts.

Generate Audit Trail Reports 208

Explains how to generate reports against application and archive databases.

Export Audit Policy 210

Explains how to export audit policies using Audit Policy Export.

Disable Auditing 211

Explains how and why to disable auditing.

Overview

Auditing is the process of evaluating an organization's practices for safeguarding electronic information from loss, damage, unintended disclosure, or denial of availability. It is one of the essential factors in providing a secure application and in meeting mandatory regulatory compliance.

The system's Auditing capability integrates with the Progress OpenEdge Auditing capability in Progress OpenEdge 10. Refer to the Progress documentation for additional information about the Auditing capability in Progress and about the Progress Data Administration utility.

With QAD's Auditing module, you can configure your system to maintain audit trails. Audit-trail records are created and stored in audit trail tables. They contain facts about changes made in the databases. A typical audit record includes information that helps you identify who made a change, which program made the change, when the change was made, and what the change was. You can set up these functions for all tables or you can limit the audit trail recording activity to specific tables.

The Auditing module adds value to the Progress OpenEdge Auditing capability by including:

- A user interface that allows you to enable and disable auditing at the table level with reusable defaults. This function is more straightforward than the audit policy maintenance function provided by Progress.
- A default audit policy. QAD's default policy includes configuration of identifying fields of tables in QAD's main database. With the default policy, users can easily identify changed records according to the content of the audit trail.
- Reports that perform better and are easier to use than the default Progress reports.
- The ability to trace the user who made the changes through the QAD architecture.
- Import/export policies to allow users to set up audit policy in one database and enforce it in other databases by exporting and importing the policy. This prevents having to repeat the setup for each database—reducing errors and ensuring that all company databases are using the same policy.

An Enhanced Controls license is required to use Auditing. Various OpenEdge utilities must also be run and data administration options set to enable particular databases for auditing.

Warning Importing policies of your own into the system or using Progress tools to change QAD's default policy may cause conflicts on policy configuration. These activities are not recommended.

Below is a list of menus and programs for the new auditing module.

Table 10.1
Auditing Module Menus and Programs

Number	Menu Label	Program
36.12.1	Audit Trail Report—App DB	atapprp.p
36.12.2	Audit Trail Report—Arc DB	atarcrp.p
36.12.13	Audit Trail Setup Menu	
36.12.13.1	Audit Policy Import	atplimp.p
36.12.13.2	Audit Policy Export	atplexp.p
36.12.13.5	Audit Configuration Maintenance	atplmt.p

Number	Menu Label	Program
36.12.13.6	Audit Configuration Report	atplrpt.p
36.12.13.11	Audit DB Maintenance	atdbmt.p
36.12.13.12	Audit DB Report	atdbrp.p

Plan Auditing

Thorough planning is necessary before setting up auditing and will save you a considerable amount of time. You should take into account certain system constraints when deciding which tables to enable for auditing. These planning considerations include:

- Which databases to audit
- Which tables to audit
- Using archive databases for reporting
- Auditing custom tables
- Schema changes

Determine Databases to Audit

Since most of the application data resides in the qaddb database, you should usually only audit-enable this database. However, you must also audit-enable the qadadmin database if you want to audit EDI tables such as the following:

- edtr_mstr
- edtrd_det
- edtrf_mstr
- edtrp_mstr
- edtrv_mstr
- edtxe_det
- edval_mstr
- edxf_mstr
- edxfd_det
- edxfdd_det
- edxfs_mstr
- edxfsd_det
- edxfsdd_det
- edxr_mstr
- edxrd_det
- edxref_mstr

Note The qadhelp database should not be audited since it only contains static system data.

Determine Tables to Audit

Most tables can be audited. However, some tables, such as those with a field type of raw or blob, cannot be audit-enabled due to technical limitations. For example, OpenEdge will generate a serious runtime error if you try to audit-enable any table with a field of the raw or blob data type. The system prevents you from enabling such tables for auditing, whether they are standard or custom tables. Audit Configuration Maintenance (36.12.13.5) will not show such tables and therefore cannot be audit-enabled. The same applies to Audit Configuration Report (36.12.13.6). As a result, you cannot see such tables in the report.

Note It is not necessary to audit tables of temporary usage within the system, such as qad_wkfl.

You might have to consider the performance overhead when deciding which tables to audit. The overhead depends on how many tables are audit-enabled and how often they change. As a rough guide, enabling auditing can cause the disk I/O for a table to increase two to three times. You usually only audit-enable those tables needed to meet your auditing requirements.

Before you audit-enable tables in a production database, QAD suggests that you validate your table audit selections in a test environment. This could include running simple tests to verify the data you need to audit is correctly collected and reported. This can eliminate unnecessary impact on your application if your table audit selections do not work as expected. If the test results are satisfactory, you can export the QAD main policy and load it into your production database.

Archive Database Considerations

You must set up the archive database to store the audit trail data to prevent the application database from growing unnecessarily large. Loading audit trail data into a dedicated archive database also has the advantage that it will not impact the performance of the application database when a lengthy audit report is generated from a separated database. You might consider distributing the audit trail data across a number of databases by date range. For example, you can create one archive database for each month, quarter or year, depending on the volume of audit trail generated in a particular period.

Auditing Custom Table Considerations

Auditing custom tables is just like auditing the standard tables—provided that the custom table schema follows QAD’s convention. The primary keys should be meaningful data items so that they can serve as identifying fields for audit trail. Again, the only constraint is that you cannot audit-enable a table with any field of data type raw or blob.

Set Up Auditing

To set up auditing, you must load the license for Enhanced Controls and then do the tasks described in the following sections:

- “Enable Auditing for the Database” on page 199
- “Configure Database Options and Audit Permissions” on page 199
- “Import Audit Policy” on page 201
- “Enable Auditing on Selected Tables” on page 202
- “Enable Auditing on Selected Fields” on page 203

Note When setting up auditing, QAD recommends that you first set up a test environment to test the auditing policy and then export the policy and load it into the production database.

Enable Auditing for the Database

In most cases, enable auditing on the database and archive database with these commands:

```
> yab -deactivateidx database-qadddb-auditing-enable
> yab database-qadarc-auditing-enable
```

For the generic case, all databases are preconfigured with database areas to store auditing data and indexes. To enable auditing on all databases, execute the command:

```
> yab database-auditing-enable
```

Alternatively, to enable auditing on a specific database, execute the command:

```
> yab database-[INSTANCE]-auditing-enable
```

Non-primary indexes are deactivated by default to improve performance when using database auditing. Deactivated indexes may be activated using `PROUTIL IDXBUILD`. The non-primary indexes are useful for reporting and can be activated on your audit archive database.

If you have activated non-primary indexes and want to deactivate them again, execute the command:

```
> yab -deactivateidx database-[INSTANCE]-auditing-enable
```

Note The database must be offline to enable auditing.

Configure Database Options and Audit Permissions

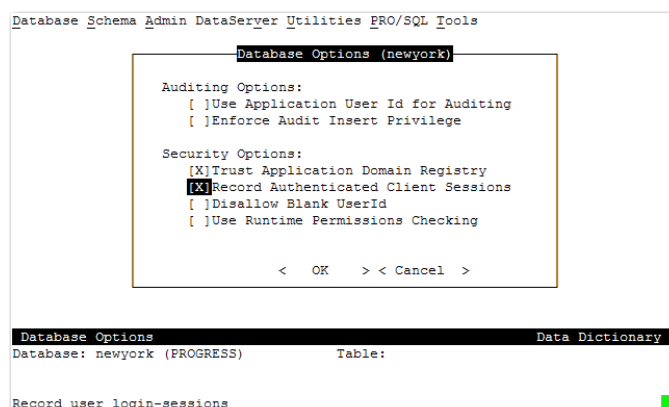
The default setup grants audit permissions to the operating system account that created the instance. In a production environment, follow the guidance in this section.

For each of the databases you have updated and enabled for auditing, you need to configure the new database options and set up audit permissions.

Note To avoid the need to restart AppServers and the WebSpeed broker, you should sign in to the database in single-user mode to perform any audit administration activities, such as defining database options. Otherwise, since the options are cached by the client for the current session, any changes you make will not take effect without restarting the system.

You set up the new database options in Progress using the Data Administration menu's Admin|Database Options settings.

Fig. 10.1
Database Options Settings



Select the following options:

- Trust Application Domain Registry
- Record Authenticated Client Sessions

To access audit-related menus, the user must be granted with specific audit permissions or roles. The roles are as follows:

- Audit Administrator — an authenticated user who has been granted privileges to create, update, and delete audit policies and read audit data.
- Audit Data Archiver — an authenticated user who has been granted privileges only to archive or load audit data. An audit data archiver has no access to the audit policy.
- Audit Data Reporter — an authenticated user who has been granted privileges to read the audit data.

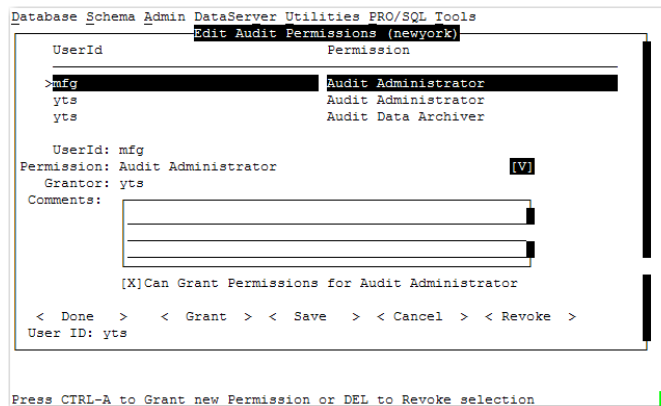
Note The Audit Administrator is not an Audit Data Archiver or Audit Data Reporter. The Audit Administrator role does not include the other roles.

Table 10.2
Roles Required for Audit Menu Access

Program	Menu	Role Required
Enhanced Controls Menu	36.12	N/A
Audit Trail Report –App DB	36.12.1	Audit Data Reporter
Audit Trail Report–Arc DB	36.12.2	Audit Data Reporter
Audit Trail Setup Menu	36.12.13	N/A
Audit Policy Import	36.12.13.1	Audit Administrator
Audit Policy Export	36.12.13.2	Audit Administrator
Audit Configuration Maintenance	36.12.13.5	Audit Administrator
Audit Configuration Report	36.12.13.6	Audit Administrator
Audit DB Maintenance	36.12.13.11	None
Audit DB Report	36.12.13.12	None

To grant audit permissions, you can use the Progress Data Administration menu's Admin|Security|Edit Audit Permissions menu.

Fig. 10.2
Edit Audit Permissions Menu

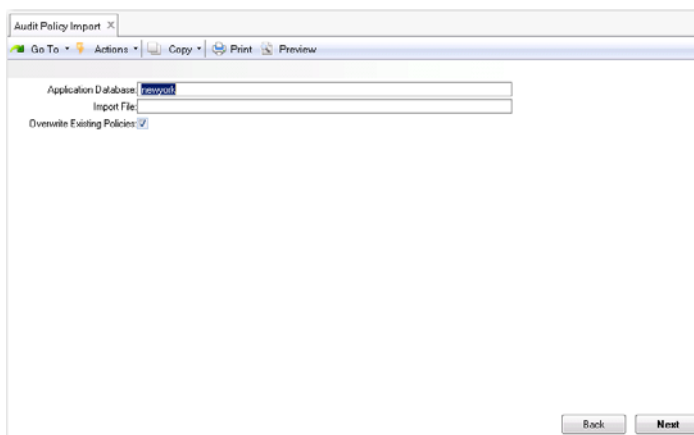


From this menu, you can reassign responsibility for the audit administration from the DBA to a separate audit administrator, and you can specify who can read and archive the audit data. For example, you might grant a particular user the Audit Administrator, Audit Data Archiver, and Audit Data Reporter permissions. (For further information, refer to the Progress documentation.)

Import Audit Policy

You can import audit policies from Progress policy XML files using Audit Policy Import (36.12.13.1).

Fig. 10.3
Audit Policy Import (36.12.13.1)



Importing audit policies only needs to be done once for each audit-enabled database. The QAD solution will not work without the Progress default policy file loaded.

To import an audit policy file, open Audit Policy Import (36.12.13.1) and complete the following fields:

Application Database. Specify the logical name of the database where the policy will be applied.

Import File. Specify the location of the XML file containing the policy definition. Two files are normally loaded: a Progress policy file that defines general settings and the QAD policy file that defines settings relevant to application tables. The two files are *installdir\config\auditing\policies.xml* (for the default settings of general activities such as sign in and changing schema) and *installdir\config\auditing\qadmainpolicy.xml* (default policy).

The reason you need a default policy (*qadmainpolicy.xml*) is as follows. When a table is audit enabled, an audit trail is created when a record is changed (an insert, modify, or delete). Important values in the audit trail include the values of identifying fields, which are used to identify the record. These values are displayed in an audit trail report and must be meaningful so that you can recognize a changed record without using database utilities. By default, Progress uses primary keys as identifying fields. If for a given table the primary key is not appropriate for identifying fields, identifying fields for the table need to be set. The default policy provides predefined identifying fields. When you use QAD's Auditing module, you should load the default policy so that you do not need to define the identifying fields.

The default policy only covers tables whose identifying fields are different from primary keys. For most non-Financials tables, the primary keys can be used as identifying fields, so these tables do not appear in the default policy. For most Financials tables, however, the table has a primary key, which is a sequence identifier, and one or two unique indexes. One unique index is used for the identifying fields. Therefore, a Financials table and its identifying fields are included in the default policy.

Overwrite Existing Policies. Select Yes to replace current policies.

Enable Auditing on Selected Tables

Use Audit Configuration Maintenance (36.12.13.5) to enable auditing on selected tables.

Fig. 10.4
Audit Configuration Maintenance (36.12.13.5)

To enable auditing on selected tables, first set the following fields:

Application Database. Specify the database name.

Selection Pattern. Leave this field blank to list all tables or enter a combination of letters and the asterisk symbol (*) as a wildcard to find tables based on matching. For example, to list only the tables whose names start with ab, enter *ab**.

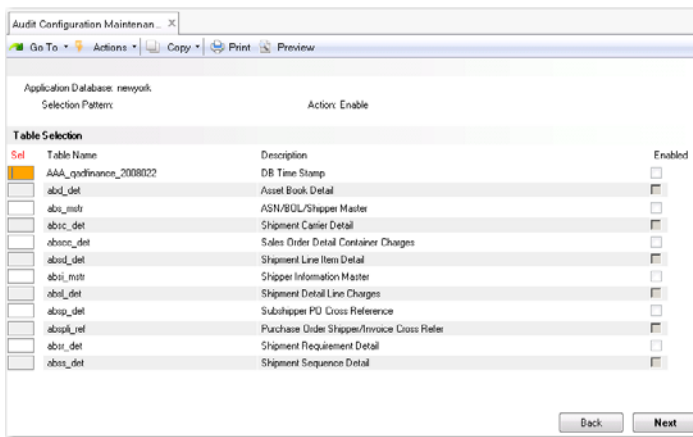
Action. Enter the code that represents the action you want to perform on selected tables:

Enable. Audit records will be created for selected tables.

Disable. Audit records will no longer be created for selected tables.

Click Next and the system lists all the tables that meet the selection pattern.

Fig. 10.5
Audit Configuration Maintenance Table Selection



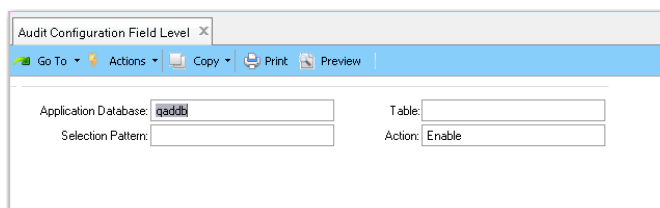
Use the up and down arrow keys to scroll through the list of tables. Use the space bar to select the tables whose Enabled settings you want to change. An asterisk symbol (*) displays at the front of the row of each table you select. To toggle the Enabled settings, select individual tables using the space bar and then press F1. The system asks whether you want to enable the selected tables. Enter Yes (or No) and then press the Enter key.

Enable Auditing on Selected Fields

You can use Audit Configuration Maintenance (36.12.13.5) and Audit Configuration Field Level (36.12.13.7) to enable auditing for specific fields and to exclude other fields.

- 1 Use Audit Configuration Maintenance to enable auditing on selected tables, as described in “Enable Auditing on Selected Tables” on page 202.
- 2 Use Audit Configuration Field Level to enable auditing for selected fields.
 - a Enable auditing for all fields in the specified table.
 - b Disable auditing for the fields you do not want to audit.

Fig. 10.6
Audit Configuration Field Level



- 3 Use Audit Policy Export (36.12.13.2) to export all policies, including qadmainpolicy.

Note You have to page down in Audit Policy Export to access and select qadmainpolicy. See “Export Audit Policy” on page 210 for more information on exporting policies.

Generate Reports for Audit Configuration

You can use Audit Configuration Report (36.12.13.6) to get a report on what tables are audit enabled/disabled and their identifying fields.

Fig. 10.7
Audit Configuration Report

To generate an audit configuration report, specify the following:

Application Database. Specify the database name.

Status. Specify the auditing status of tables (Enabled, Disabled, or All).

Table Name and To. Specify a range of table names. Typically, you leave these fields blank to get a report of all tables that meet the Status criteria.

Press Go to have the system retrieve the records according to the criteria you have specified and generate a report (or output file).

For each table that meets the criteria, the report shows the name, whether the table has been enabled for auditing, and the identifying fields.

Archive Database

The system is preconfigured with an archive database (qadarc). Audit trail data is archived to this database. The archive database is a copy of the database with auditing enabled. No other schema needs to be loaded. There are several reasons for having an archive database:

- Audit trail data requirements grow over time, requiring more disk space. Having a separate archive database prevents audit trail data from taking disk space in the application database.
- Running audit reports against the application database will impact system performance.
- The archive database can be deployed in a flexible way.
- The archive database can store audit trail data from different application databases and act as a central reporting database.

Manage the Archive Database Server

The database server for the archive database is not configured to start and stop when the environment is started and stopped.

To manually start the archive database server:

```
> yab database-qadarc-start
```

To manually stop the archive database server:

```
> yab database-qadarc-stop
```

This default can be changed with the following configuration setting:

```
build/config/configuration.properties
```

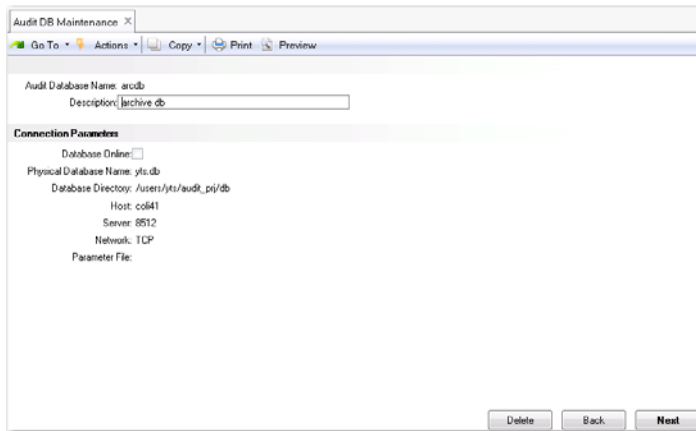
```
dbserver.qadarc.manual=false
```

In some cases an organization may want to change the default. For example, an organization may want an archive database for each month. To define a reference to an archive database, use this command:

```
> yab config audit.archive.database
audit.archive.database=db.qadarc
```

Use Audit DB Maintenance (36.12.13.11) to create and maintain connection parameters for the archive databases.

Fig. 10.8
Audit DB Maintenance (36.12.13.11)



These connection parameters are used by Audit Trail Report–Arc DB (36.12.2).

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.
- Connections to the archive databases are not permanent. The audit reports use the connection information to connect to the archive databases as needed. These processes do not maintain a connection to an archive database after they have retrieved the information they are handling.
- The system can connect to multiple archive databases simultaneously.

Important Archive databases must be configured and started up in multi-user mode before connecting to them using the connection parameters. Audit DB Maintenance does not start or stop archive databases. It only stores the connection parameters used to connect to them. You must set up external procedures to start up and shut down archive databases as needed.

Database connection parameters are defined by the way archive databases are implemented. The system administrator who creates and maintains the database provides the connection information required to set up the field values on this screen.

In the first frame, enter a name for this archive database connection record. The name must be 8 or fewer 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 archive database.

Database Online. This field indicates whether the system should attempt to connect to the archive database. It does not indicate that an archive database is running, or 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. 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.

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.

Host. Enter the name of the host server where the Progress database 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.

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.

Parameter File. Specify the parameter file name. You must specify the connection parameters either in the parameter file or in the corresponding Host, Server, and Network fields. (Do not specify them in both.) If you use the parameter file:

- The file must be accessible through the PROPATH or located in the directory specified in Database Directory.
- You must still specify the database name in Audit DB Maintenance (36.12.13.11). If the database is not located in the PROPATH, you must specify the full path in Database Directory.
- The file must not include the -ld or -db parameters.
- The file must include the -trig parameter, which specifies the location of trigger files.

Database Connection Report

You can use Audit DB Report (36.12.13.12) to get a report on the database connection and its parameters.

Fig. 10.9
Audit DB Report (36.12.13.12)

Enter the following:

Audit Database Name, To. Specify a range of database names. Typically, you leave these fields blank to get a report on the connection information of all archive databases.

Specify the output format and click Next to run the report.

Execute Archive/Load Scripts

Before auditing records can be moved from a source database into the archive database, the source database and the archive database must have auditing enabled.

To move auditing records from all databases enabled for auditing, execute the command:

```
> yab database-auditing-archive
```

Alternatively, to move auditing records out of a specific database, execute the following command, where **INSTANCE** is the name of the source database:

```
> yab database-[INSTANCE]-auditing-archive
```

The archive command consists of two steps:

- 1 Audit records are exported into a directory within `build/work/auditing`, which removes the records from the source database.
- 2 The records are loaded into the archive database.

The audit records in the work directory are not deleted when the command completes as a precaution to allow the records to be reloaded if the second step fails. If a failure occurs, you can specify the `(-audit.workdir)` option to locate the work directory containing the audit records to load. When the archive process is successful, the work directory can be removed.

The following settings configure the operation of the archive command:

```
# The account to use when archiving audit data or empty to use the
# current OS account.
#
```

NOTE: If an audit.user is not configured the 'Audit Administrator', 'Audit Data Archiver', and 'Audit Data Reporter' roles will be granted to the OS account that was used to create the database so auditing functionality works out of the box. If an audit.user is configured we assume we are working in a restricted environment where auditing authorization will be handled directly using the Progress data dictionary.

audit.user=

The password for the audit.user account.

audit.password=

The database where archived audit records will be stored.

audit.archive.database=db.qadarc

The directory where exported audit records will be stored.

audit.archive.dir=\${appdir.work}/auditing

Note If the audit.user was not defined when the environment was created, the operating system account that was used to install the environment needs to be set up as an application user to configure auditing within the application. To configure audit users and roles that provide a better segregation of responsibilities, see Configure Database Options and Audit Permissions.

Generate Audit Trail Reports

You can generate reports against application databases and against archive databases.

Generate Reports Against Application Databases

You can generate auditing reports against the application databases using Audit Trail Report–App DB (36.12.1).

Fig. 10.10
Audit Trail Report–App DB (36.12.1)

To generate audit reports, specify the following:

Application Database. Select one of the connected databases. If the database selected is not enabled for auditing, the system displays an error message.

Table Name. Specify a table, or leave this field blank to specify all tables.

User ID. Specify a user ID, or leave this field blank to specify all users.

Program Name. Specify the name of the program that changed the records. For example, specify `sosomt .p` (Sales Order Maintenance) to get audit trail data generated for changes made by Sales Order Maintenance.

Date, To. Specify the beginning and ending dates.

Summary/Detail. Select summary mode or detail mode. In summary mode, no field value changes are reported.

Output Format. Specify the output format as a text file (.txt) or XML file (.xml).

Click Next. If just one table was selected, then the system displays the identifying fields and allows the user to specify a range of values for one or more fields to narrow the search results. This frame displays the field name and the field label for each identifying field of the selected database table. You can specify from and to values in the data range frame.

Fig. 10.11
Audit Trail Report–App DB Field Selection

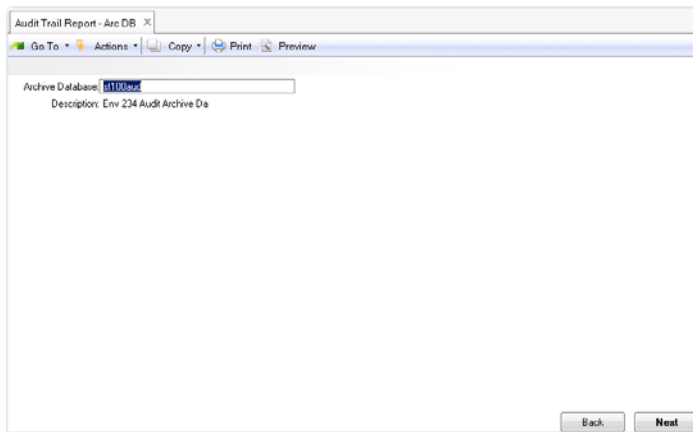
Click Next again to have the system retrieve the records according to the criteria you have specified and generate a report (or output file).

The report shows the Table Name, User ID, Date, Time, and Program for each audit trail record that meets the criteria.

Generate Reports from Archive Databases

You can generate auditing reports from the archive databases using Audit Trail Report–Arc DB (36.12.2).

Fig. 10.12
Audit Trail Report–Arc DB (36.12.2)



To generate audit reports, specify the following:

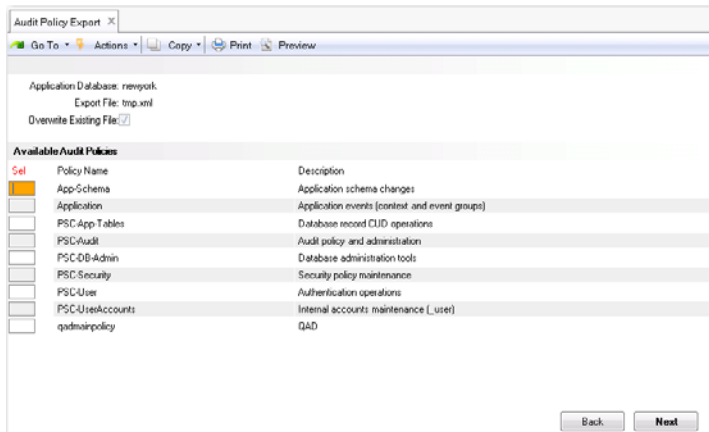
Archive Database. Select one of the archive databases. If the database selected is not enabled for auditing, the system displays an error message. Use Audit DB Maintenance (36.12.13.11) to define archive database information.

Click Next to have the system retrieve the records according to the criteria you have specified and generate a report (or output file).

Export Audit Policy

You can export current audit policies to Progress policy XML files using Audit Policy Export (36.12.13.2).

Fig. 10.13
Audit Policy Export (36.12.13.2)



To export to an audit policy file, specify the following:

Application Database. Select one of the applications databases. (If the database selected is not enabled for auditing, you will get an error message.)

Export File. Specify the name of the Progress policy XML file to which you want to export the audit policy.

Overwrite Existing File. Specify whether you want to overwrite an existing Progress policy XML file.

Click Next and the system lists all the current audit policies. Use the up and down arrow keys to scroll through the list of policies. Use the space bar to select the policies you want to export. An asterisk symbol (*) displays at the front of the row of each policy you select. Click Next (or in the Character UI, press F1) and the system prompts you to export the selected policies to the export file you have specified.

Disable Auditing

As an audit administrator, you can disable auditing for a database, but the database must be offline when you disable auditing for that database. Disabling auditing does not remove any recorded audit data or the auditing tables. Access to the audit data remains restricted to authorized users when auditing is disabled.

To disable auditing on all databases with auditing enabled, execute the command:

```
> yab database-auditing-disable
```

To disable auditing on a specific database, execute the command:

```
> yab database-[INSTANCE]-auditing-disable
```


Reverse Proxy for Channel Islands

This section covers the following topics:

Overview 214

Explains the security benefits of using a generic proxy.

Configuration 214

Explains how to configure the proxy controller.

Overview

Exposing any application to the internet greatly increases the security risks faced by that application. To provide secure access to external web applications, you can use a QAD-supplied generic proxy that hides external applications behind a firewall, ensuring that the secure Channel Islands UI controls access to those applications.

Configuration

The Proxy Controller is configured in `qad-webshell.properties`.

Proxy Configuration

Each external application has a name, as well as a local path from which to proxy, and a remote server to which to proxy:

Table 11.1
Proxy Configuration

Property	Description
<code>qad-webshell.proxy.names</code>	Comma-separated list of proxy names. These are then used as keys for the other properties in this table.
<code>qad-webshell.proxy.{name}.proxyFrom</code>	The path from which to proxy; for example, <code>/remote</code> must start with a <code>/</code> . The full proxy path is generated from this value as <code>{context}/proxy{proxyFrom}</code> .
<code>qad-webshell.proxy.{name}.proxyTo</code>	The URL to which to proxy; for example, <code>https://remote.qad.com/context</code> .

Note If the external application is hosted at the root of the remote server, you must include a forward slash, `/`, at the end of the `proxyFrom` and `proxyTo` parameters. For example, to proxy to the Tomcat default application `https://tomcat-internal.qad.com:22000`, use:

```
proxyFrom=/tomcat/ and proxyTo= https://tomcat-internal.qad.com:22000/
```

Without this forward slash, relative links on the page may not be resolved correctly.

URL Rewriting

With a reverse proxy, it is often necessary to rewrite URLs in the proxied content to be consistent with the local path. For example, the local path `/qad-webshell/proxy/app` is proxied to the remote server `https://remote.qad.com/context`, and the proxied content contains links similar to the following

```
<a href="https://remote.qad.com/context/some/cool/api">Click Me!</a>
<a href="/context/some/cool/api">Click Me!</a>
```

Without rewriting, the first link would try to bypass the proxy and go directly to the remote server. The second link would resolve as:

```
https://webshell.qad.com/context/some/cool/api
```

when it should instead be:

```
https://webshell.qad.com/proxy/app/some/cool/api
```

The solution to these problems is URL rewriting. Currently, QAD supports rewriting for HTML (html), JavaScript (js), and JSON (json) content. To enable content rewriting with default settings, add the following property with a comma-separated list of rewriters:

```
qad-webshell.proxy.{name}.rewriters
```

For example,

```
qad-webshell.proxy.{name}.rewriters=html,json
```

HTML Rewriting

Links in HTML can occur in one of the following places:

- Inside an HTML attribute: `<a href="URL">`
- Inside an HTML event handler: `<body onload="load('URL')">`
- Inside styles attribute or content: `<div style="background-image: url('URL')">` or `<style> { background-image: url('URL'); }</style>`
- Inside script content: `<script>var url = 'URL'</script>`

Enabling the HTML rewriter enables only attribute rewriting by default. To enable and configure link, event, style, and script rules, add the following property with a comma-separated list of rewrite options:

```
qad-webshell.proxy.{name}.rewriters.html
```

Each option works by applying a set of rewrite mappings to selected content in the HTML document. Each option has the following default behavior.

link

The link option is responsible for rewriting links in HTML attributes. By default, it looks for links in href, src, action, data, and cite attributes. It applies a set of rewrite mappings to those attribute values in the document. Rewrite mappings are either simple mappings that match and replace a given prefix, or regex mappings that perform general match and replace. The default mappings are based on the proxy configuration. For example, suppose proxyFrom=/app, proxyTo=https://remote.qad.com/path, and the webshell context is qad-webshell. Two simple mappings are defined:

```
/path -> /{context}/proxy/app
https://remote.qad.com/path -> /qad-webshell/proxy/app
```

event

The event option is responsible for rewriting links in HTML event handlers. By default it looks for links in the following attributes:

- onclick
- ondblclick
- onmousedown

- onmouseup
- onmouseover
- onmousemove
- onmouseout
- onkeypress
- onkeydown
- onkeyup
- onfocus
- onblur
- onload
- onunload
- onsubmit
- onreset
- onselect
- onchange

Because the event handler can contain arbitrary JavaScript, this option uses regex mappings by default to look for links in JavaScript strings. Using the same scenario as in the link example, suppose proxyFrom=/app, proxyTo=https://remote.qad.com/path, and the webshell context is qad-webshell. The default mappings are defined:

```
'(?:https://remote\.qad\.com/path|/path)((?:[^\\"|]|\\.)*)' -> '/qad-webshell/proxy/app$1'
"(?:https://remote\.qad\.com/path|/path)((?:[^\\"|]|\\.)*)" -> "/qad-webshell/proxy/app$1"
```

style

This option rewrites links in script attributes and script content. By default, it uses the following regex mappings to match CSS URL data types:

```
url(\s*'(?:(?:https://remote\.qad\.com/path|/path)((?:[^\\"|]|\\.)*)' \s*\s*) -> url('/qad-webshell/proxy/app$1')
url(\s*"(?:(?:https://remote\.qad\.com/path|/path)((?:[^\\"|]|\\.)*)" \s*\s*) -> url("/qad-webshell/proxy/app$1")
```

script

This option rewrites links in script content. By default, it uses the same regular expressions as the event option.

The default behavior for each of these options can be customized using the following properties.

Table 11.2
Script Content Properties

Property	Description
qad-webshell.proxy.{name}.rewriters.html.{option}.attributes	Comma-separated list of attributes for link and event options. Include 'default' in the list to use default attributes in addition to custom ones.
qad-webshell.proxy.{name}.rewriters.html.{option}.mappings	Comma-separated list of mapping types to apply. Current supported values are 'simple,' 'regex,' and 'default'

Property	Description
qad-webshell.proxy.{name}.rewriters.html.{option}.mappings.simple	Simple rewrite mappings in pairs separated by spaces. For example, /path /qad-webshell/proxy/app https://remote.qad.com/path /qad-webshell/proxy/app
qad-webshell.proxy.{name}.rewriters.html.{option}.mappings.regex	Regex mappings in pairs separated by spaces. For example, '(?:https://remote\.qad\.com/path/path)((?:[^\s\\] \\\.)*)' /qad-webshell/proxy/app\$1' \"(?:https://remote\.qad\.com/path/path)((?:[^\s\\] \\\.)*)\" /qad-webshell/proxy/app\$1"

Example

In this example, two proxy endpoints are set up:

- /qad-webshell/proxy/configurator -> https://procon-internal.qad.com:16560/procon
- /qad-webshell/proxy/tomcat/ -> https://tomcat-internal.qad.com:22000/

The Tomcat proxy has URL rewriting enabled for HTML links with custom attributes and mappings. The qad-webshell.properties file would look like the following:

```
qad-webshell.proxy.names=tomcat,configurator
qad-webshell.proxy.configurator.proxyFrom=/configurator
qad-webshell.proxy.configurator.proxyTo=https://procon-internal.qad.com:16560/procon
qad-webshell.proxy.tomcat.proxyFrom=/tomcat/
qad-webshell.proxy.tomcat.proxyTo=https://tomcat-internal.qad.com:22000/
qad-webshell.proxy.tomcat.rewriters=html
qad-webshell.proxy.tomcat.rewriters.html=link
qad-webshell.proxy.tomcat.rewriters.html.link.attributes=href,src,action,value
qad-webshell.proxy.tomcat.rewriters.html.link.mappings=simple
qad-webshell.proxy.tomcat.rewriters.html.link.mappings.simple=/qad-webshell/proxy/tomcat/
```

Configuring Caching of Java Objects

The Channel Islands UI caches Java objects using the Ehcache Java caching library. Caches used by a plugin are configured in entries in the properties file of the plugin. The properties include:

- <plugin name>.cacheNames: CSV list of cache names that should be initialized for use by the plugin, without the plugin name prefix.
- <plugin name>.cache.<cache name>.maxEntriesLocalHeap: Maximum number of objects that will be cached in memory (0 = no limit).
- <plugin name>.cache.<cache name>.maxEntriesLocalDisk: Maximum number of objects that will be maintained in the DiskStore (0 = no limit).
- <plugin name>.cache.<cache name>.eternal: Indicates if timeouts are ignored and the element is never expired (true/false).
- <plugin name>.cache.<cache name>.timeToIdleSeconds: Maximum amount of time between accesses before an element expires (0 = no limit).

- `<plugin name>.cache.<cache name>.timeToLiveSeconds`: Maximum time between creation time and when an element expires (0 = no limit).
- `<plugin name>.cache.<cache name>.persistence`: The persistence strategy to use. Only two options are available, `localTempSwap`, which configures the cache to overflow to disk, or `none`.
- `<plugin name>.cache.<cache name>.memoryStoreEvictionPolicy`: Least recently used (LRU), First in first out (FIFO), or Less frequently used (LFU).

All properties except `<plugin name>.cacheNames` are optional, defaulting to the corresponding values from the central `ehcache.xml` configuration file defined in the `qad-webshell-webui` plugin at:

`src/main/resources/com/qad/webshell/config/ehcache.xml`.

The use of a particular cache can be disabled by changing the `<plugin name>.cacheNames` property to remove the cache name. However, any cache annotations referencing that cache must also be removed, or else an exception will be thrown at run time when the WebShell is started.

Disk Store Configuration

The Ehcache DiskStore is used for additional cache storage and persistence. In newer versions of Ehcache the disk store is configured globally per CacheManager, rather than per cache. By default, `java.io.tmpdir` will be used, however this can be configured in `qad-webshell.properties` as follows:

```
qad-webshell.cacheManager.diskStorePath=//host/path/to/disk/store #Linux
```

```
qad-webshell.cacheManager.diskStorePath=\\\\host\\path\\to\\disk\\store #Windows
```

Refresh Ahead Caching

As of version 2.7, Ehcache provides a Refresh Ahead cache decorator that can improve cache performance by asynchronously refreshing cache entries. The refresh ahead cache is configured with a time-to-refresh (TTR) value, in addition to time-to-live (TTL) and (optional) time-to-idle (TTI) values. A refresh is triggered when a non-expired cache entry is accessed if more than TTR seconds have elapsed since creating of the cache. For example, suppose we set TTR=30s, TTL=60s, and no TTI. Then, any cache entry that is accessed between 30s and 60s after creation will trigger the asynchronous refresh.

Refresh ahead caching is configured in the plugin's properties file using the following options:

- `<plugin name>.cache.<cache name>.decorators`: CSV list of decorators to apply to the cache. Currently, the only supported option is `refreshAhead`.
- `<plugin name>.cache.<cache name>.refreshAhead.timeToRefreshSeconds`: The number of seconds an entry can exist in the cache before it is refreshed on access. Expired items that have yet to be evicted cannot be refreshed. (REQUIRED.)
- `<plugin name>.cache.<cache name>.refreshAhead.maximumBacklogItems`: The maximum number of refresh requests allowed in the refresh work queue. Once this limit is exceeded, items are dropped from the queue to prevent potentially overtaxing resources. (REQUIRED.)

- `<plugin name>.cache.<cache name>.refreshAhead.batchSize`: The maximum number of refresh requests that can be batched for processing by a thread. For more frequent processing of requests—at a cost to performance—lower the value. Defaults value is 100.
- `<plugin name>.cache.<cache name>.refreshAhead.numberOfThreads`: The number of threads to use for background refresh operations on the decorator. Defaults value is 1.
- `<plugin name>.cache.<cache name>.refreshAhead.evictOnLoadMiss`: Force an immediate eviction on a reload miss (true) or to not evict before normal eviction takes effect (false). Default value is false.

Product Information Resources

QAD offers a number of online resources to help you get more information about using QAD products.

[QAD Forums \(community.qad.com\)](https://community.qad.com)

Ask questions and share information with other members of the user community, including QAD experts.

[QAD Knowledgebase \(knowledgebase.qad.com\)*](https://knowledgebase.qad.com)

Search for answers, tips, or solutions related to any QAD product or topic.

[QAD Document Library \(documentlibrary.qad.com\)](https://documentlibrary.qad.com)

Get browser-based access to user guides, release notes, training guides, and so on; use powerful search features to find the document you want, then read online, or download and print PDF.

[QAD Learning Center \(learning.qad.com\)*](https://learning.qad.com)

Visit QAD's one-stop destination for all courses and training materials.

*Sign-in required

Index

Symbols

! (exclamation point) 108
.NET UI security 23
* (asterisk) 108

Numerics

2.14.1 53
36.3.1 51
36.3.3 20
36.3.4 59
36.3.6.1 66
36.3.6.2 66
36.3.6.3 66
36.3.6.4 66
36.3.6.5 14, 67, 148
36.3.6.6.1 15, 70
36.3.7.1 116
36.3.7.2 117
36.3.7.3 118
36.3.7.5 119
36.3.7.6 120
36.3.7.8 120
36.3.7.9 121
36.3.7.13 121
36.3.7.14 122
36.3.7.15 122
36.3.7.17 122
36.3.13.1 123
36.3.13.2 123
36.3.13.8 112
36.3.13.13 124
36.3.13.14 124
36.3.15.1 110, 111
36.3.15.2 111
36.3.15.3 110
36.3.15.4 110
36.3.22 59
36.3.23.1 19, 33
36.3.23.12 56
36.3.24 26
36.5.3.24 108
36.12.4 189
36.12.5 190
36.12.7 192
36.12.1 208
36.12.13.8 169, 184
36.12.13.1 201
36.12.13.11 205, 206, 210
36.12.13.12 206
36.12.13.2 210
36.12.13.5 202, 203

36.12.13.7 203
36.12.14.1 178
36.12.14.4 169, 178
36.12.14.5 179
36.12.14.9 184
36.12.14.21 192
36.12.14.22 169, 193
36.12.14.23 169, 193
36.12.2 205, 209
36.16.10.1 58
36.24.1 19
36.6.1 205

A

Activated E-Signature Profile Report 184
Activated Field Security Report 110
Active field 54
address
 e-mail specification 55
administrator
 security e-mail 32
Administrator Role field 28
API type
 User Maintenance 54
application resource 3
applications
 assigning 58
Archive SOD log records 162
archive/delete
 e-sig failures 192
 e-signatures 169, 193
Assigning segregation of duties categories 142
Audit Configuration Field Level 203
Audit Configuration Maintenance 202, 203
audit databases
 archiving electronic signatures 193
Audit DB Maintenance 205, 206, 210
Audit DB Report 206
Audit Policy Export 210
Audit Policy Import 201
audit profiles
 groups 178
 overview 177
Audit Trail Report - App DB 208
Audit Trail Report - Arc DB 205, 209
Auditing 196
Auto-Disablement Reason field 29

C

categories, electronic signature 170
checklists

- security implementation 7
- committing data to database 186
- compiles
 - protecting in Progress 22
- component-based functions 3
- control programs
 - security 26
- country
 - information in locale.dat file 53
 - setting country code for user 53
- Country Code Data Maintenance 53
- County Code field 53
- Ctrl+F display 28
- Current field 185
- Customer type
 - User Maintenance 54

D

- data
 - committing to database 186
- Data Administration (Progress) 199
- data dictionary
 - field security 110
- Database Connection Maintenance 205
- Database Control 19
- databases
 - Progress security 22
- DBAUTHKEY function in Progress 22
- deactivated roles 66
- default domain 60
- default role 62
- delete/archive
 - e-sig failures 192
 - e-signatures 169, 193
- dependencies 86
 - Show Dependencies check box 86
- Dictionary Field Security Report 109, 110
- DO Receipts Restriction Maintenance 122
- DO Restriction Maintenance 121
- DO Shipments Restriction Maintenance 122
- domains
 - default 60
 - security access 17, 59

E

- electronic signature categories 170
- electronic signature profiles
 - activating 184
 - refreshing 178
 - updating in workbench 179
- electronic signatures 164, 193
- e-mail
 - auditing notifications 187
 - electronic signature notifications 170
 - notification settings 28
 - security notifications 32
 - user's address 55
- employee type
 - User Maintenance 54
- enabled reason code 56
- Enabled Reason field 56
- Enabled Reason Type field 29
- Enabled setting 56
- Enforce Licensed User Count 27, 57

- Enforce OS User ID 27
- Enhanced Controls license 196
- entity security 59
- errors
 - license violations 27
- E-Sig Failure Archive/Delete 192
- E-Signature Archive/Delete 169, 193
- E-Signature Events Report 189
- E-Signature Failure Report 192
- E-Signature Group Maintenance 178
- E-Signature History Report 190
- E-Signature Profile Activation 169, 184
- E-Signature Restore 169, 193
- E-Signature Workbench Profile Maintenance 179
- E-Signature Workbench Refresh 169, 178
- exceptions
 - segregation of duties policy 149
 - SOD policy 149
- Export SOD data to Excel 154
- Export SOD data to XML 157

F

- field security 92, 109
 - validation 110
- Field Security by Role 111
- Field Security Maintenance 110, 111
- filters, electronic signature 175, 181, 183
- Force Password Change field 56
- Force Password Change Utility 56
- functions
 - component-based 3

G

- general ledger (GL)
 - account security 123
- GL Account Security Maintenance 123
- GL Account Security Report 123
- gppswd.v 110
- groups
 - auditing 178
 - electronic signature 178

H

- Header Display Mode field 27

I

- Import SOD data from Excel 155
- Import SOD Data from XML 158
- inactive records 54
- interface preferences 55
- International Organization for Standardization (ISO)
 - codes 53
- Inventory Detail Restriction Maintenance 117
- Inventory Movement Code Security 124
- Inventory Movement Code Security Browse 124
- Inventory Transfer Restriction Maintenance 116
- inventory update 112–123
- Invoice Post
 - site security 112

L

- Language field
 - User Maintenance 53
- languages

- identifying for users 53
- length
 - password minimum 30
- License Registration 58
- licensing
 - interaction with User Maintenance 57
 - tracking violations 27
 - warnings versus errors 27
- locale.dat file 53
- log files
 - segregation of duties 162
- Logon Attempt Report 19, 33

M

- material requirements planning (MRP)
 - site security 112
- Maximum Access Failures field 28
- membership
 - role 15, 70
- menu substitution
 - User Maintenance 55
- menu-eligible resource 76
- menus 76
 - role 76

N

- .NET UI security 23
- node states 69

O

- operating system
 - security 20–??
 - using ID for application sign in 20
- Operational Transaction Post 59

P

- passwords
 - creation method 31
 - forcing change 56
 - managing 16
 - Security Control settings 30
 - updating 57
- permissions
 - role 14
- PO Receipts Restriction Maintenance 120
- PO Restriction Maintenance 119
- Primary location for user access 54
- Product Change Control (PCC)
 - using electronic signatures with 187
- programs
 - standard 3
- Progress
 - blank user ID 21
 - compiles, protecting 22
 - database schema controls 22
 - DBAUTHKEY function 22
 - Editor security 21
 - RCODEKEY function 22
 - schema controls 22
 - security 20
- Progress Editor
 - access 21

Q

- QAD type
 - User Maintenance 54

R

- RCODEKEY function in Progress 22
- reason codes
 - active reason 29
 - electronic signatures 169
 - enabled reason 56
- record-locking during signature entry 181
- records
 - active 51
 - inactive 54
- registered applications
 - assigning 58
- reports
 - electronic signatures 189
- resource
 - application 3
- Resource spreadsheet 153
- role context 70
- Role Create 66
- Role Delete 66
- role membership 15
- role membership compliance 128
- Role Membership Maintain 15, 70, 148
- role menu 76
- Role Modify 66
- role permissions compliance 128
- Role Permissions Maintain 14, 67, 148
- Role View 66
- role-based access control 14–??, 48
- roles 14, 61
 - deactivated records 66
 - default 62
 - deleting 66
 - system-supplied 64

S

- Sales and Use Tax Interface (SUTI)
 - controlling access 108
- Sarbanes-Oxley (SOX) Act 2
- schema
 - controlling in Progress 22
- security
 - client level 22
 - Dictionary Field Security Report 109
 - domain 17
 - field 109
 - field limitations 110
 - GL accounts 123
 - implementation checklists 7
 - implementation summary 6
 - inventory movement code 124
 - monitoring 33
 - overview 3
 - Progress Editor 21
 - schema level 22
 - site 112
 - special characters 109
 - types of 4
 - wild cards 108
 - Windows systems 23

- Security Control 26
- segregation of duties (SOD)
 - planning SOD system 131
 - setup workflow 129
- Segregation of duties categories 140
 - definition 128
- Segregation of duties matrix 144
- Segregation of Duties Menu 129
- Session Expires Minutes field 27
- sign in
 - security 17
 - tracking attempts 33
 - using operating system user ID 20
- signature meaning 169
- Single Sign-On Enabled field 29
- site security 112
 - excluded functions 112
 - ranges of sites 113
 - setting up 113
- Site Security Maintenance 112
- SO Restriction Maintenance 120
- SO Shipments Restriction Maintenance 121
- SOD Block All Rule Violations 146
- SOD Block All Rule Violations field 128, 132, 133, 134, 139, 151
- SOD Block All Violations field 146
- SOD Category Create 140
- SOD Category Delete 140, 141
- SOD Category Excel Integration 141
- SOD Category Membership Maintain 142, 144
- SOD Category Modify 140
- SOD Category View 140
- SOD Category worksheet 142, 152
- SOD Configuration 128, 132, 133, 134, 138, 146, 151
- SOD Import/Export 151
- SOD Log Archive 162
- SOD Log Delete/Archive 162
- SOD Log Viewer 158, 162
- SOD Matrix Maintain 144
- SOD Matrix worksheet 152
- SOD Policy Exception Create 149
- SOD Policy Exception Delete 150
- SOD Role Exclusion 150
- SOD Violations Rule 1 View 161
- SOD Violations Rule 2 View 161
- SSM Restriction Maintenance 122
- standard programs 3
- states
 - node 69
- System Access frame
 - User Maintenance 56
- system roles 64

T

- Tax Interface Control 108
- time zone
 - setup 54
- Time Zone field 54

- Timeout Minutes field 22, 26
- top tables, electronic signature 174
- tracking
 - sign-in attempts 33
- transaction scoping 186
- tree nodes 69

U

- Unplanned Issue/Receipt Restriction Maintenance 118
- update restrictions 113
 - wildcards 114
- User Access by Application Inquiry 59
- User Domain/Entity Access Maintain 59
- user ID
 - assigning 51
 - blank, in Progress 21
 - displaying at user interface 28
 - setting up 51
- User Maintenance 51
 - country code 53
 - interface preferences 55
 - language 53
 - locale 53
 - QAD type 54
 - System Access frame 56
 - time zone 54
 - Variant field 53
- user name
 - viewing 28
- User Password Maintenance 20
- User Type field 54
- users
 - defining types 54
 - e-mail address 55
 - enforcing license agreement 57
 - interface preferences 55
 - locale 53
 - time zone 54
 - violation messages for license agreement 57

V

- Variant field
 - User Maintenance 53

W

- warning messages
 - license violations 27
- wildcards
 - update restrictions 114
 - use with security 108
- Windows security options 23
- workflow
 - electronic signatures setup 166
 - security setup 6
 - segregation of duties setup 129
- workspace security 17