Security Administration Guide

QAD Adaptive Applications

70-3349-2024QAE
QAD Adaptive ERP 2024
August 2024

Security_AG_v2024QAE.pdf/sti/ymg/su9/su9/su9

QAD Inc.
100 Innovation Place
Santa Barbara, California 93108
Phone (805) 566-6000
https://www.qad.com

Contents

Security Admin Guide Change Summary xiii

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 11

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 17
Sign-in Security 18
Workspace Security 18
Sign In and Security Control 19
OS-Based Sign-in Security 20
Operating System and Progress Security 22
Progress Editor Access 22
Progress-Level Database Schema Controls 23
Compiling Custom Code on Unprotected Databases 23
Client-Level Security 25
Windows Systems 25
Non-Windows Systems 25
QAD Adaptive ERP Security 26

Chapter 3 Security Control 27

Define General Security Settings 28
Create a Password Strategy 32
Set Up Email Notifications 34
Monitor System Security 35

Chapter 4 Secured Configuration 37

Overview 38
Prerequisites 38
Certificates 39
Keystores and Truststores 39
Enabling SSL/TLS 40
Configure Tomcat to Enable SSL/TLS 41
Setting Up a Secured Configuration 41
Platform Runtime Service 42
Key Management Service 42
Enable the Key Management Service 42
Encrypt Content 43
Disable the Key Management Service 43
KMS Backup and Recovery 43
Database Security 43
Enable Database Security 44
Connection User 44
Transparent Data Encryption (Optional) 45
Enable SSL for AppServerDCS 47
Enable HTTPS for Progress AppServer 48
Securing Data in Transit 49
Tomcat Configuration 50
OpenEdge Database Configuration 50
Adaptive UX Support for Encryption 50
Adaptive UX Tomcat Maintenance Mode 51
Maintenance Mode Timeout Setting 51
Security with Apache Kafka (Optional) 51
Enable SSL on the Kafka Server Side 52
Enable SSL on the Kafka Client Side 52
SSL Client Authentication 52
Credentials Authentication 53
Security with Apache Cassandra (Optional) 53
Enable SSL 53
Enable SSL Client Authentication 54
Credential Authentication 54
Security with Apache NiFi 55

Nifi Troubleshooting 56

Chapter 5 Authentication 57

Overview 58
User Authentication 58
LDAP Authentication 58
Internal 58
Directory Services Markup Language Service 58
Configure Java Keystore 59
Install DSML Gateway 59
Review and Update Directory to QAD Database Mappings 61
Download QAD Adaptive ERP 64
Configure SYNC reason code 64
Configure Alternate Country Code 64
Configure LDAP Instance 65
Verify LDAP Instance Definition for DSML Gateway Using User Sync 65
Test LDAP 69
API Authentication 69
Smart Card Authentication 70
Define Properties 71
SAML Single Sign-On 74
Required Properties for SAML SSO 74
SAML Endpoints 78
Single Sign-On to QAD Adaptive ERP 79
SAML SSO Troubleshooting 81

Chapter 6 Users and Roles 85

Overview 86
Role and User Definition Process Workflow 86
Set Up Roles 88
Uses of Roles 88
Define Roles 93
Create a New Adaptive ERP Role 94
Create a New Adaptive UX Role 95
Copy an Adaptive UX Role 96
Copy and Merge Adaptive UX Roles 98
Define Role Permissions 101
Set Up Users 104
User Synchronization 105
Types of Users 105
Define Users 106

Specify Access to Domains and Entities 115
Define Role Membership 119
QAD Adaptive ERP Role Membership Maintain 119
QAD Adaptive UX User Access Roles Grid 120
View Access Information 121
Export and Import Roles and Permissions 121
Role and User Audit Reports 123

Chapter 7 Adaptive UX Security 127

Overview 128
Prerequisites 128
Role and User Workflow in Adaptive UX 128
Resources 128
Adaptive UX Resources 128
Menus 129
Role Menus 129
Favorites Menu 133
Copy and Merge Multiple Menus 135
Role Permissions 136
Permission Propagation, Inheritance, and Configuration 137
Resource Dependencies 143
Role Permissions Actions 144
Assigning Permissions to Roles 146
Role Menu Dependency 153
Troubleshooting Role Permissions 154
Resource Permission Types 154
Role Resource Audit Report 155
Configure Stored Views Access 157
Record-Level Security 158
Configuring Security Rule Properties 159
Enabling Record-Level Security 159
Granting Access to Records 161
Reapply Security Rules 168
Secure Records Browse 169

Chapter 8 QAD Adaptive ERP Security. 173

SSH on the QAD Adaptive ERP 174
Public Key Authentication for SSH 175
SSH for QAD Adaptive ERP Terminal Mode 177
HTTPS for QAD Adaptive ERP Desktop Screen Display 177
HTTPS for AIA 178
SSL for AppServerS and AppServerDCS 179

Additional Security for Standard Programs 181
Specifying User IDs and Roles 182
Limiting Access to Fields 183
Controlling Inventory Updates 185
Defining GL Account Security 197
Defining Inventory Movement Code Security 198

Chapter 9 Segregation of Duties in Adaptive ERP 199

Overview 201
Segregation of Duties Verification 202
Segregation of Duties Compatibility Matrix 203
Segregation of Duties Policy Exceptions 203
Segregation of Duties Process Workflow 203
Plan a Segregation of Duties System 205
Segregation of Duties Rule Checking 206
Role Permissions Validation 206
Role Membership Validation 207
Direct and Indirect Violations 208
Segregation of Duties Rule Matrix 209
Complete Prerequisite Activity 212
Disable the Superuser Role 212
Activate Segregation of Duties 212
Activate Segregation of Duties from QAD Adaptive ERP 212
Activate Segregation of Duties from the Command Line 214
Maintain Segregation of Duties Categories 214
Delete Categories 216
SOD Category Excel Integration 216
Assign Resources to Segregation of Duties Categories 218
Assigning Resources in QAD Adaptive ERP 218
SOD Category Membership Excel Integration 220
Maintain the Segregation of Duties Matrix 221
SOD Matrix Excel Integration 223
Define Role Permissions 224
Define Role Membership 225
Maintain Segregation of Duties Policy Exceptions 225
SOD Policy Exceptions 226
Segregation of Duties Role Exclusions 227
Import and Export Segregation of Duties Data 228
SOD Category Worksheet 229
SOD Matrix Worksheet 229
Resource Worksheet 230
Role Worksheet 230
Export to Excel 231

Import from Excel 232
Export to XML 234
Import from XML 235
Report and View Logs and Violations 235
View Log History 235
Report on Current Segregation of Duties Conflicts 236
View Role Permissions Violations 238
Archive Log Record Files 239

Chapter 10 Segregation of Duties in Adaptive UX. 241

Overview 243
Segregation of Duties Verification 244
Segregation of Duties Compatibility Matrix 245
Segregation of Duties Policy Exceptions 245
Segregation of Duties Process Workflow 245
Plan a Segregation of Duties System 247
Segregation of Duties Rule Checking 248
Role Permissions Validation 248
Role Membership Validation 249
Direct and Indirect Violations 250
Segregation of Duties Rule Matrix 251
Complete Prerequisite Activity 254
Disable the Superuser Role 254
Activate Segregation of Duties 255
Maintain Segregation of Duties Categories 256
Assign Resources to Segregation of Duties Categories 257
Assigning Resources 258
Define Role Permissions 260
SOD Role Permissions Comparison Report 261
Define Role Membership 262
Maintain Segregation of Duties Policy Exceptions 262
SOD Policy Exceptions 262
Segregation of Duties Role Exclusions 264
SOD Setup 264
SOD Categories 265
SOD Matrix 266
Roles 266
Import and Export Segregation of Duties Data 267
Export to Excel from SOD Setup 269
Import to SOD Setup 271
Report and View Logs and Violations 272
View Log History 272
Report on Current Segregation of Duties Conflicts 272

View Role Permissions Violations 274
Archive Log Record Files 275

Chapter 11 Electronic Signatures in Adaptive ERP 277

Overview 278
Electronic Signature Enabled Programs 278
Programs for Electronic Signature Setup and Reporting 280
Electronic Signature Planning Steps 281
Electronic Signature Workflow 281
Set Up Electronic Signature Functionality 283
Load Electronic Signature Initial Data 283
Set Up Electronic Signature Reason Codes 283
Define Security Control Settings 284
Electronic Signature Categories 285
Category Considerations 287
Tables and Fields 288
Filters 289
Electronic Signature Profiles 291
Overview 291
Define Electronic Signature Profiles 292
Create Signature Groups 293
Refresh Signature Profiles 293
Update Signature Profiles 295
Activate Electronic Signature Profiles 299
Record Electronic Signatures 300
Transaction Scoping 302
Product Change Control 302
Email Notifications 303
Signature Profile Activation Email 303
Signature Failure Email 303
Reporting 304
Setup Reports 304
Electronic Signature Records for Quality Control 305
Electronic Signature Reports 305
Functional Reports and Inquiries 308
Archive and Restore Records 309

Chapter 12 Electronic Signatures in Adaptive UX. 311

Overview 312
Electronic Signature Planning Steps 312
Electronic Signature Workflow 313
Set Up Electronic Signature Functionality 313

Set Up Electronic Signature Reason Codes 314
Define Security Control Settings 314
Define Electronic Signature Configurations 315
E-Signature History 320
Record Electronic Signatures 322
E-Signature Modes 322
E-Signature UI Mode 325
E-Signature API Mode 325

Chapter 13 Auditing 329

Overview 330
Plan Auditing 331
Determine Databases to Audit 331
Determine Tables to Audit 332
Archive Database Considerations 332
Auditing Custom Table Considerations 332
Set Up Auditing 333
Create Generalized Codes to Enable CSV Output 333
Enable Auditing for the Database 333
Configure Database Options and Audit Permissions 334
Import Audit Policy 337
Enable Auditing on Selected Tables 338
Enable Auditing on Selected Fields 339
Generate Reports for Audit Configuration 340
Archive Database 340
Manage the Archive Database Server 341
Database Connection Report 343
Execute Archive/Load Scripts 343
Generate Audit Trail Reports 344
Document Audit Trail Reports 345
Generate Reports Against Application Databases 349
Generate Reports from Archive Databases 350
Export Audit Policy 351
Disable Auditing 352

Chapter 14 Reverse Proxy for QAD Adaptive ERP 353

Overview 354
Configuration 354
Proxy Configuration 354
URL Rewriting 354
Configuring Apache Reverse Proxy Timeout Setting 358
Configuring Caching of Java Objects 358

Disk Store Configuration 359
Refresh Ahead Caching 359

Chapter 15 Menu Search Implementation 361

Overview 362
Elasticsearch Settings 362
Troubleshooting 362

Appendix A KMS Backup and Recovery 365

Overview 366
KMS Backup 366
KMS Zip File 366
Data File 366
KMS Recovery 367

Appendix B Logi Platform Services 369

Logi Platform Services Network Ports 370
HTTPS Certificates 371
Creating HTTPS Certificates 371
Configuring Certificate Files and Location 371
Apache Reverse Proxy Configuration for LogiPS 371
Logi Platform Services Product Database Security 372

Index. 375

Security Admin Guide Change Summary

Product Name Changes

Starting in September 2019, the new name for QAD's complete portfolio of products is QAD Adaptive Applications. Additionally, QAD Adaptive ERP is the new name for QAD's flagship ERP solution. QAD Adaptive ERP includes the functionality previously associated with QAD Cloud ERP and QAD Enterprise Applications - Enterprise Edition, plus the QAD Enterprise Platform and Adaptive UX, which resulted from the Channel Islands program. Going forward, the terms QAD Enterprise Applications, QAD Cloud ERP, and Channel Islands will be deprecated but will remain in previous documentation and training materials. QAD's intention is to—as soon as possible—eliminate the use of the deprecated terms going forward.

Change Summary

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

Date/Version	Description	Reference
August 2024/QAD Adaptive ERP	Added the *Enable HTTPS for Progress AppServer* section.	page 48
March 2024/QAD Adaptive ERP 2024	Deleted the *Languages and Locales* section.	--
	Updated the *Role Permissions* section.	page 136
	Added the *E-Signature Modes* seAugust 2024ction.	page 322
March 2023/QAD Adaptive ERP 2023	Updated the *Adaptive UX Security* chapter	page 127
September 2022/QAD Adaptive ERP 2021.1	Added a new *Copy an Adaptive UX Role* section	page 95
	Added a new *Copy and Merge Adaptive UX Roles* section	page 98
January 2022/QAD Adaptive ERP 2021.1	Updated information on entering database names on Auditing DB Maintenance.	
December 2021/QAD Adaptive ERP 2021.1	Added information on disabling autofill of credentials in web browsers as part of electronic signature setup.	page 313
	Updated the recommended process for granting audit permissions.	page 336
	Introduced a description of audit reports and included details on available user and role reports.	page 346, page 123, and page 155

Date/Version	Description	Reference
September 2021/QAD Adaptive ERP 2021.1	Added details on the settings that must be secured for the Platform Runtime Service.	page 42
	Added information on the new action for importing EE role permissions into Adaptive UX.	page 145
	Moved Adaptive UX segregation of duties content to its own chapter and improved the directions for importing and exporting segregation of duties data using Excel integration.	page 241
	Introduced a new chapter for electronic signatures in Adaptive UX.	page 311
	Added a new section on out-of-the-box audit trail reports.	page 345
March 2021/QAD Adaptive ERP 2021	Updated the Segregation of Duties chapter to include expanded Adaptive UX functionality, including SOD Setup, SOD Categories, Excel import and export integration, and an OpenEdge setting that is required for activation.	page 199
	Adaptive UX Tomcat Maintenance Mode	page 51
	Added configuration information for securing Apache Nifi.	page 55
December 2020/QAD Adaptive ERP 2020.1 Rev 1	Adding information on importing browses and QRF reports into Adaptive UX using the Import Secure Resources action.	page 144
September 2020/QAD Adaptive ERP 2020.1	Revised Database Security section in a secured configuration.	page 43
	Added a section on enabling SSL for AppServerDCS.	page 48
	Introduced section on security with Apache Kafka.	page 51
	Introduced section on security with Apache Cassandra.	page 53
	Added information on securing the NiFi port.	page 55
	Added a section on troubleshooting role permissions.	page 146
	Revised Stored Views Access information to reflect ability to now configure stored views access in Adaptive UX.	page 157
	Added a description of the new action to reapply security rules.	page 168
	Updated Segregation of Duties chapter to include new Adaptive UX screens and functionality.	page 201
May 2020/QAD Adaptive ERP 2020 Rev 1	Clarified that multi-factor authentication is available through third-party identity providers when SAML is enabled.	page 5
	Minor updates to clarify Secure Configurations.	page 37
	Included information for companies using self-signed certificates.	page 39
	Updated the steps required to disable KMS.	page 43
	Added details on the required OAuth 2 Password grant parameters.	page 69
	Clarified that KMS backup files should be stored separate from the host environment.	page 366

Date/Version	Description	Reference
March 2020/QAD Adaptive ERP 2020	Updated product portfolio naming.	--
	Updated LDAP Distinguished Name information to allow for special characters and to escape commas in usernames.	page 66
	Added Sync Users option user synchronization in the QAD Adaptive UX.	page 68
	Introduced new property to enable SAML SSO.	page 75
	Added information for Full Access selection in Permissions Grid.	page 144
	Introduced Resource Permission Types browse in the QAD Adaptive UX.	page 154
	Updated Record Level Security Owner information.	page 158
	Introduced updated timeout setting for Apache Reverse Proxy.	page 358
	Added an appendix to explain Logi Platform Service integration with QAD Adaptive UX.	page 369
October 2019/QAD 2019EE Rev 2	Removed support for enabling SSL/TLS on AppServers for securing data in transit.	--
September 2019/QAD 2019EE Rev 1	Clarified that users must be assigned to roles in both Adaptive UX and the Adaptive ERP in order to access the different interfaces.	page 93 and page 119
	Highlighted that Mobile App users must be assigned to the webui_user role.	page 118
	If you enable database security and are using auditing, you must have a parameter file that includes the username and password that were used to secure the database.	page 342
September 2019/QAD 2019EE	Introduced a chapter explaining how to securely configure your system from end to end with a key management service, database security and OpenEdge TDE, along with securing data in transit.	page 37
	Added new timeout property for SAML SSO.	page 75
	Reorganized chapters 6 and 7 to reflect continued advancements in Adaptive UX capabilities with users and roles.	page 85 and page 127
	Elasticsearch can now be used in production environments to better handle large numbers of documents and searchable documents.	page 361
	Added Appendix A to describe backup and recovery of a key management service.	page 365
March 2019/2018EE with QAD Cloud ERP 2019	Explained how to enable single sign-on to QAD Adaptive ERP when using the QAD Adaptive UX.	page 79
	Introduced record-level security functionality for the QAD Adaptive UX.	page 158
	Added generalized code creation for CSV file format option.	page 333
	Added CSV file format option for auditing reports.	page 344
	Added instructions for enabling SSL for AppServerDCS.	page 179

Date/Version	Description	Reference
September 2018/2018EE	Removed information for single sign-on and Enforce checkboxes from Security Control.	Chapter 3
	Updated information on enabling SSL.	page 40
	Added information on implementing smart card authentication.	page 70
	Added SAML single sign-on information.	page 74
	Created an appendix that lists the fields that can be secured in the QAD Adaptive UX.	page 355
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 32
	Created a new chapter on authentication.	page 57
	Significant updates to Chapter 7, “Adaptive UX Security,” including user and role information, role permissions, menus, and resources.	page 127
	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 28
	Added a section on Active Directory	page 111
	Added chapter on setting up secured Channel Islands resources	page 127
	Added chapter on setting up reverse proxies for Channel Islands	page 353
	Changed the directory where QAD-provided default profiles are found	page 283
	Updated some sections in the Auditing chapter	page 329
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 277
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 212
	Added new section on Activating Segregation of Duties from the Command Line	page 214
	Various minor changes	--
March 2013/2013 EE	Updated description for Timeout Minutes field	page 28
	Updated description for User ID field	page 107
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 90
	BCube activity removed from Secured Items Not on Menu table.	page 90
	BReportTree activity removed from Secured Items Not on Menu table.	page 90

Date/Version	Description	Reference
	BDInvoice node with activity Customer Invoice–Modify Due Date [Entity] added to Secured Items Not on Menu table.	page 90
	BERS and BERSLine activities added to Secured Items Not on Menu table.	page 90
	Generalized Code Groups added to Secured Items Not on Menu table.	page 91
	New section added on Enabling Auditing on Selected Fields.	page 339
September 2011/2011.1 EE	Rebranded for QAD 2011.1 EE	--

Chapter 1

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 11
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 Adaptive 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 QAD Adaptive ERP.

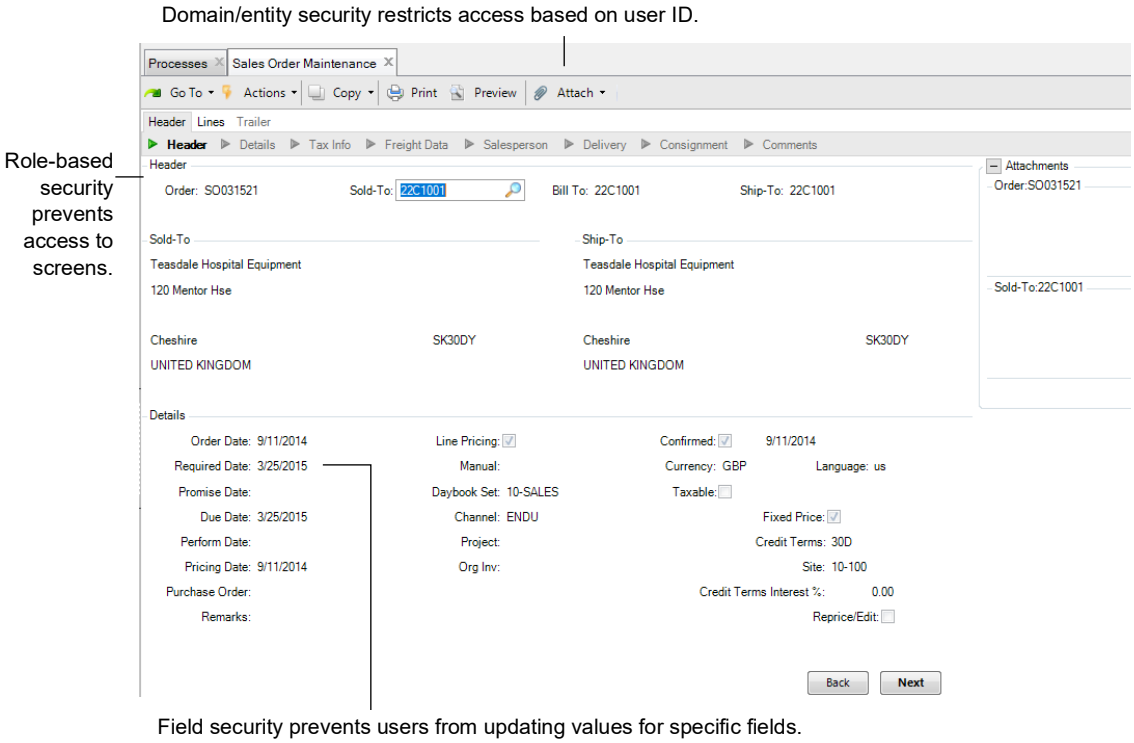
Additionally, Adaptive UX is comprised of multiple types of resources, which are uniquely identifiable pieces of the product that have been designated as needing to be secured. These resources include business entities, services, browses, fields, and KPIs.

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, QAD Adaptive ERP, or the QAD Adaptive UX.

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 22 for details.

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

Fig. 1.1
Types of Security



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 collection of roles (for example, roles defined in QAD Enterprise Edition) within the Directory service.
- 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.

Web Application Features

- SAML single sign-on can be enabled.
- HTTPS is the standard protocol.
- OAuth 2 compliant, including support for APIs.
- Form-based login to Adaptive UX.
- Field security can be enabled.
- Support for record-level security at the business component level.
- Multi-factor authentication is supported through third-party identity providers when SAML is enabled.
- Support for X.509 certificate login.
- Support reauthentication requests for tasks that require additional user verification.

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:

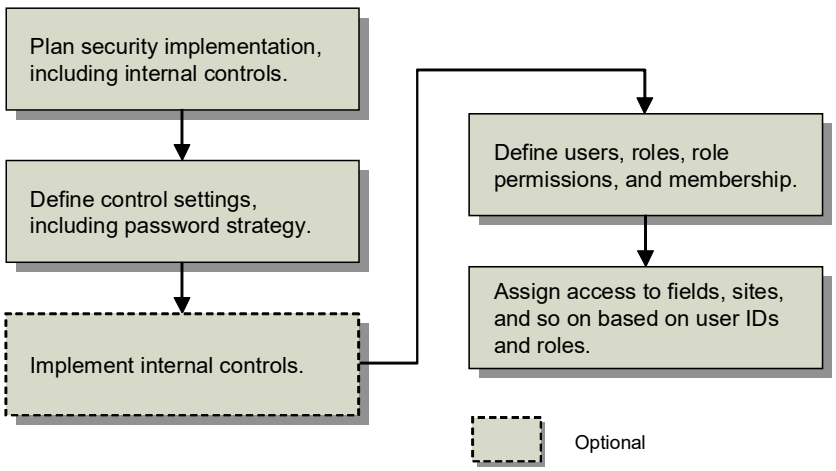
- Segregation of duties. Provides features that prevent a user from participating in more than two parts of a transaction or process. This is accomplished by partitioning the system application resources into mutually exclusive categories. See Chapter 9, "Segregation of Duties in Adaptive ERP," on page 199.

- 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 11, “Electronic Signatures in Adaptive ERP,” on page 277.
- 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 13, “Auditing,” on page 329.

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 92.

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 8.

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 27.
- 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 85.
- 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 181 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 • *Installation Guide* • Progress documents, including *Data Administration, Guide*, *Client Deployment Guide*, and *Programming Handbook*
Review all application-related files to determine the appropriate permission and ownership settings.	"Operating System and Progress Security" on page 22
Optionally, determine and document any segregation of duties policy requirement. Also document how application resources should be partitioned.	Setting Up Segregation of Duties
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 106 • "Specify Access to Domains and Entities" on page 115
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 88
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 181
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 104
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 205
Determine procedures to be used to create new user accounts and communicate initial passwords (email, personal contact, other).	"Create a Password Strategy" on page 32
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 changed passwords, and update the corresponding system security setting.	"Expiration Days" on page 33

Topic	Reference
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 email notification • Reviews of system logs • Procedures for resetting locked accounts	• "Security Control" on page 27 • "Monitor System Security" on page 35
Define password policies and procedures, including password composition, length, expiration, and reuse of previous passwords.	"Create a Password Strategy" on page 32
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 25

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 23
Consider disallowing Progress-level table and field access for the blank user ID	"Progress Editor Access" on page 22
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 25
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 27
Define users assigned to the security administrator role, who will receive email notification of security events such as failed logins exceeding a defined threshold.	• "Administrator Role" on page 30 • "Maximum Access Failures" on page 30
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 32

Topic	Reference
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 181
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 QAD Adaptive ERP (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
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	mgurrp.p

Program No.	Description	Program Name
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
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

Chapter 2

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 ***17***
Describes how passwords can be managed using Security Control settings.

Sign-in Security ***18***
Outlines types of sign-in, domain and workplace security, and different types of security control.

Operating System and Progress Security ***22***
Describes different types of operating system and progress security, including details on Progress Editor and Progress-level database information.

Client-Level Security ***25***
Describes potential client-level security settings that are available with some operating systems.

QAD Adaptive ERP Security ***26***
Explains how QAD Adaptive ERP 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 Adaptive UX.

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 QAD Adaptive ERP or Role Permissions in Adaptive UX.

- 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 Adaptive ERP Security" on page 173 and "Adaptive UX Security" on page 127.

The QAD Adaptive ERP 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 Adaptive ERP and User Access in Adaptive UX 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 181.

Additional Security for Adaptive UX

The system has additional security for Adaptive UX. This security, which is defined by role, is managed through Adaptive UX.

- 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.
- QAD Adaptive ERP is designed to operate over the internet with a secure UI and secure APIs.
- All actions in Adaptive UX are determined by role security.

For details on setting Adaptive UX security, see “Adaptive UX Security” on page 127.

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 32.

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 email 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 113.

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 22 for details.
- Domain/entity security limits individual user access to the domains and entities identified in User Domain/Entity Access Maintain (36.3.4). Using Adaptive ERP 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, QAD Adaptive ERP, and Adaptive UX. 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 Adaptive ERP and Adaptive UX, the authentication service creates a session for the user, and returns a session ID to Adaptive ERP. Adaptive ERP 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 Adaptive ERP can be successful even when the user is not assigned to a workspace. This is because Adaptive ERP 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 Adaptive ERP and Adaptive UX, 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 Adaptive ERP, 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 115.

When a user exits Adaptive ERP, 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 Adaptive 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 checkbox remains active in Security Control, but you should not select it. If you do select the checkbox, you will receive Active Directory errors and be prompted for sign-in credentials.

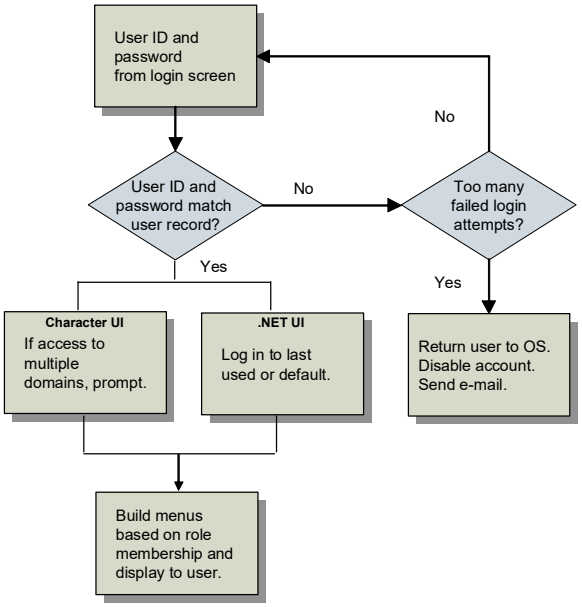
If a user enters an invalid combination of user ID and password, the system may prompt additional times—based on the value of Maximum Access Failures in Security Control. After the specified number of failures, the user is returned to the operating system, the user account is disabled, and system administrators are notified by email. The sending address of the email 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 Adaptive ERP and Adaptive UX 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 Adaptive ERP and Adaptive UX must enter a valid user ID and password to access the system.

When the Enforce OS User ID checkbox 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 checkbox 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 checkbox, the system displays a message to warn you of a potential security compromise. In addition, if using the Adaptive ERP, 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.

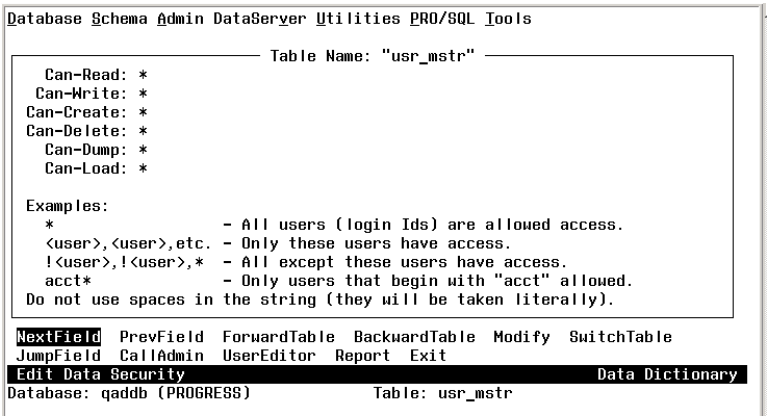
Another related control that should be considered is to disallow privileges for users connecting to the application database with a blank user ID. The Disallow Blank User ID Access option on the Progress Database|Admin|Security menu is available for this purpose. See the “Maintaining Application Security” 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 28.

In the character UI, this feature applies only when the application is displaying a menu, rather than when a program is executing. In the Adaptive ERP, 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 Adaptive ERP. 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 Adaptive ERP Security

The QAD Adaptive ERP 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.

Chapter 3

Security Control

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

Define General Security Settings ***28***
Describes the frames of Security Control and what they are used for.

Create a Password Strategy ***32***
Describes how to use the Password frame to specify password settings, such as complexity requirements and expiration dates.

Set Up Email Notifications ***34***
Describes the circumstances under which the system can automatically send email notifications to users.

Monitor System Security ***35***
Describes the automatic features used to help administrators control and monitor security activities.

Define General Security Settings

You can define security settings in both Adaptive ERP and Adaptive UX. The Security Control screens in both interfaces contain the same settings, though in different orders. The following screen shots depict Adaptive ERP.

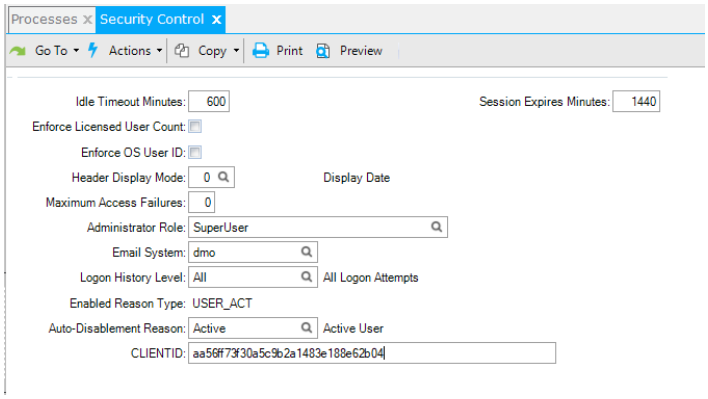
Use the two frames of Security Control (36.3.24) to:

- 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 Email Notifications” on page 34 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. Values can range from 0 through 9,999 minutes.

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 25 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 Adaptive ERP, 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 Adaptive ERP.

- This setting does not affect Adaptive UX. Adaptive UX timeout is determined by values defined in Tomcat settings.

Session Expires Minutes. This field indicates how long the session can be used before it expires, in minutes. 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.

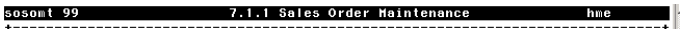
Header Display Mode. Use this field to control the information that displays in the menu and program title bars of programs in the character interface. Valid values are:

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 email message to the system administrator. See "Set Up Email Notifications" on page 34 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 34 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 34 for details.

Typically, the administrator role includes a primary system administrator and one or more alternates.

Email System. Specify an email 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 email definition specified for the signed-in user in User Maintenance. If the user record does not include a valid email definition, the one specified in this field is used. For more information on setting up email, see *QAD System Administration User Guide*.

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 35.

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 112 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).

Create a Password Strategy

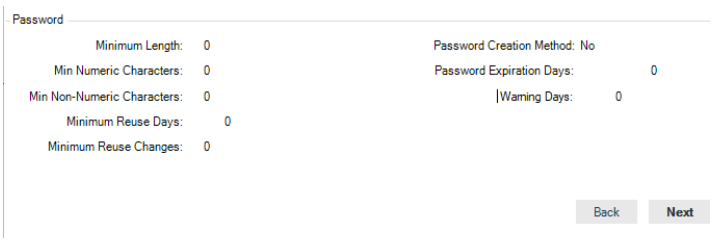
Use the Password frame to define the complexity requirements and expiration time period for user account passwords. Anytime a new password is created for an account—either manually or automatically—that password must meet the rules you set up here. Use as many or as few password parameters as required 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 checkbox 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 checkbox and specify password parameters as needed. See “OS-Based Sign-in Security” on page 20.

Fig. 3.6
Security Control, Password Frame



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 35.

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.

Note Non-numeric characters that are valid in passwords include the following: ~!@ #$%^&*(_+|":}>?<[;'\./,-=`)].

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 113.

- 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 Email Notifications” on page 34.

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 in 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 Email 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 emails to members of an administrator role. The email 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 email was automatically generated from an application process. If you have any
  questions about this email, contact the system administrator. Do not reply to this email.
  ```

- When Password Creation Method is set to Email in the Password frame of Security Control, the system generates a new password and emails it to the user based on the email address specified in User Maintenance. This occurs for new and existing users when the Update Password checkbox is selected in User Maintenance. The email text is similar to the following:

  ```
  The purpose of this email is to inform you of your new temporary application password.
  You have been sent this email because Security Control has been set up to email
  autogenerated temporary passwords.

  Your temporary application password is: password.
  You will be forced to change this password at next logon.

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

- When any field or checkbox is updated in Security Control, the system generates and sends emails to members of the administrator role. The email 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 email 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.

Chapter 4

Secured Configuration

This section describes how to configure your system to secure all aspects of your data both at rest and in transit.

Overview ***38***
Describes the system components that can be secured.

Prerequisites ***38***
Explains certificates and keystores.

Enabling SSL/TLS ***40***
Describes the steps necessary to enable SSL/TLS for Tomcat.

Setting Up a Secured Configuration ***41***
Outlines the process of securing your system from end to end.

Platform Runtime Service ***42***
Explains the properties that must be configured to secure the Platform Runtime Service.

Key Management Service ***42***
Explains the properties that must be configured to enable KMS.

Database Security ***43***
Explains the properties that must be configured to enable database security.

Enable SSL for AppServerDCS ***47***

Provides the properties to configure security for all AppServers.

Enable HTTPS for Progress AppServer ***48***

Provides the properties to configure security for Progress AppServers, which supports OpenEdge version 12 and is available for Adaptive ERP 2024 users.

Securing Data in Transit ***49***
Explains the properties that must be configured to secure and encrypt data in transit.

Adaptive UX Support for Encryption ***50***
Provides the information necessary for Adaptive UX to decipher encrypted data.

Security with Apache Kafka (Optional) ***51***

Security with Apache Cassandra (Optional) ***53***

Security with Apache NiFi ***55***

Overview

QAD Adaptive ERP supports security features applied to its components, which ensures data is secure both at rest while on the file system and while in transit. System security is applied in layers, allowing you to set up end-to-end system security all at once or in stages. QAD recommends you enable security for your production environment.

QAD Adaptive ERP supports the following security features:

SSL/TLS. All Tomcat instances support secure communication using SSL/Transport Layer Security (TLS).

Key Management Service. A key management service (KMS) is a lightweight micro-service that provides API endpoints to secure secret information such as passwords, client secrets, and API keys.

Database Security. Within a QAD environment, you can secure OpenEdge databases in two ways.

- Authentication/Authorization, which restricts access at the database or database table level. Users are required to enter a username and password before they can log in to an OpenEdge database.
- Transparent Data Encryption, which provides block-level encryption of data while it is at rest in the file system.

Data in Transit. Data in transit is protected by transferring information encrypted with SSL/TLS. The components that can use SSL/TLS to encrypt data are:

- Tomcat servers
- OpenEdge databases

Apache Kafka Security. Apache Kafka is used for building real-time data pipelines and streaming apps. You can secure Kafka connections by encrypting data.

Apache Cassandra Security. Apache Cassandra is a key component in the Adaptive UX Action Centers and you can secure Cassandra connections by encrypting data.

QAD recommends reviewing this chapter in its entirety before implementing any of the security features described in it. Only skilled system administrators should enable this functionality. Contact QAD Support or Services for assistance.

Prerequisites

Your environment must have QXtend and Alerts packages with versions that are at least equal to the following.

- qxtend-bundled=1.9.2.4
- alerts-bundled=1.3.3.9

Next, acquire a signed certificate for your server and import that certificate into the server keystore and the keystores of the other components you are securing. These instructions assume all components are located on the same server.

Certificates

A secured configuration requires at least one X.509 certificate that digitally binds a cryptographic key to an organization's details. For a certificate to work without warnings, it must be signed by a trusted third party, known as a Certificate Authority (CA). After you have chosen a CA, follow their directions to procure a certificate. If you are using self-signed certificates, make sure you also configure the appropriate truststores.

Keystores and Truststores

A keystore is a repository of security certificates and private keys, which are often stored using aliases. Generally, a keystore holds certificates and keys that identify and are used to authenticate the server on which the keystore is located.

A truststore is also a repository of certificates, but its certificates identify trusted external clients and servers that want to communicate with the client on which the truststore is located. A Java truststore is distributed in a file named "cacerts." Cacerts contains the most common publicly available CAs.

Keystore for OpenEdge Server

The OpenEdge root certificate store is located in the `OpenEdge-Install-Dir\certs` directory. For detailed information on setting up the keystore and importing a certificate, refer to Progress documentation on managing OpenEdge certificate stores and on using the certutil utility.

Java Keystore

The QAD default keystore is a Java keystore and can only be used with Java components. The configuration for the default keystore is defined when QAD Adaptive ERP is installed, and the keystore is created when the first certificate is imported. For security reasons, QAD recommends changing the default password before importing a certificate. For detailed information on keystores, see Java documentation.

The QAD default configuration associates all Tomcat instances with the default keystore (keystore.default) that is located in `build/work/keystore/default.bin`. You can change the location of the keystore by configuring the setting `keystore.default.file`.

To find the keystore with which the Tomcat instance is associated, enter:

```
> yab config tomcat.default.keystore
tomcat.default.keystore=/dr01/qadapps/qea/build/work/keystore/default.bin
```

To view the configuration of the default keystore, which includes the default password, enter:

```
> yab config keystore.default.*
keystore.default.file=/dr01/qadapps/qea/build/work/keystore/default.bin
keystore.default.password=changeit
```

To find the configurable properties for QAD keystores, enter:

```
yab help keystore
```

Change the Java Keystore Password

Change the keystore password before importing certificates into the keystore. If the password is changed after the certificates are imported, the certificates must be imported again. To change the password, update the following setting in `configuration.properties`.

```
keystore.default.password=<abetterpassword>
```

After you update the password, remove the existing keystore. If the keystore does not exist, nothing will be done.

```
> yab keystore-default-remove
```

Import Certificates into the Java Keystore

The X.509 certificate must be imported into the keystore that is associated with the Tomcat instance to be secured. If you are importing multiple certificates into the keystore, you can use an alias to uniquely identify the certificates. Tomcat uses the first certificate in the keystore unless the certificates are configured with an alias. You should use aliases when importing certificates for various QAD instances, such as Adaptive UX, the QAD Adaptive ERP Home server, the Event Service, and QXtend.

To import a certificate without an alias, enter:

```
yab keystore-default-import -key:<PRIVATE KEY> -certificate:<CERTIFICATE
CHAIN>
```

To import a certificate with an alias, enter:

```
yab keystore-default-import -key:<PRIVATE KEY> -certificate:<CERTIFICATE
CHAIN> -alias:cert1
```

For more information, use the command help:

```
yab help keystore-default-import
```

Reverse Proxy

If you are using a reverse proxy, refer to “Reverse Proxy for QAD Adaptive ERP” on page 353.

Enabling SSL/TLS

SSL/TLS is enabled for QAD by configuring Tomcat. Ensure you have a signed certificate that has been imported into the default Java keystore before proceeding.

For an overview of SSL, 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

Configure Tomcat to Enable SSL/TLS

Configure the following setting to true to enable SSL/TLS and disable http on a Tomcat instance:

```
tomcat.<INSTANCE>.usessl=true
tomcat.<INSTANCE>.usehttp=false
```

For example:

```
tomcat.webui.usessl=true
tomcat.qxtend.usessl=true
tomcat.default.usessl=true
```

If you have multiple certificates in the Java keystore, you can use the following setting to identify the alias of the certificate to use:

```
tomcat.<INSTANCE>.keyalias=<ALIAS>
```

For example,

```
tomcat.default.keyalias=cert1
```

To apply the change, update the Tomcat instance.

```
yab tomcat-<INSTANCE>-update
```

Setting Up a Secured Configuration

The following process outlines the steps to take to secure your system from end to end.

1. Stop your environment.

   ```
   yab stop
   ```

2. Open the `build/config/configuration.properties` file.
3. Configure the platform runtime service. See “Platform Runtime Service” on page 42.
4. Configure the key management service. See “Key Management Service” on page 42.
5. Configure database security. See “Database Security” on page 43.
6. Configure Tomcat servers and OpenEdge databases to secure data in transit. See “Securing Data in Transit” on page 49.
7. Enable security for Apache Kafka. See “Security with Apache Kafka (Optional)” on page 51.
8. Enable security for Cassandra. See “Security with Apache Cassandra (Optional)” on page 53.
9. Enable Adaptive UX to decrypt data. See “Adaptive UX Support for Encryption” on page 50.
10. Update your environment.

    ```
    yab update
    ```

Platform Runtime Service

The Platform Runtime Service (PRS) extends the Progress runtime with Java logic and executes platform business logic. The service requires ZeroMQ 4, which must be installed on the server. See the *Adaptive UX On-Premise Installation Guide* for details.

You can control and monitor the PRS using a REST API. To secure that REST API, configure the following settings:

```
prs.server.ssl.enabled=true
prs.server.ssl.key-store-type=JKS
prs.server.ssl.key-store=/<path to keystore>/keystore.jks
prs.server.ssl.key-store-password=<password for keystore>
prs.server.ssl.key-alias=<SSLCertificateAlias>
```

Key Management Service

A Key Management Service (KMS) is a lightweight micro-service that provides API endpoints to secure secret information such as passwords, client secrets, and API keys through encryption. Adaptive UX works with the KMS by recognizing encrypted data and calling the KMS to decrypt that data when it receives encrypted properties.

QAD Adaptive ERP supports encryption between the KMS and Adaptive UX. This includes integration with Tomcat instances in which sensitive data from the Tomcat `server.xml` file is externalized and encrypted using the KMS.

Important Do not use YAB setting references to KMS encrypted properties. For example, setting `foo=${tomcat.webui.keystorepassword}` would set `foo` to an encrypted value, which other parts of the application that reference this value may not be able to decrypt. Using references instead of explicit property values can lead to unexpected behavior.

Enable the Key Management Service

A KMS instance is installed during QAD Adaptive ERP installation. The system creates a client ID and configures the KMS. You must have a certificate configured for the KMS for the system to successfully update. For information on keystores and certificates, see the section “Java Keystore” on page 39.

Note If your KMS and Tomcat server are running on the same system, you can use the same certificate for both components.

To enable the KMS, define the following KMS properties in the `configuration.properties` file.

```
kms.server.ssl.key-store-type=JKS
kms.server.ssl.key-store=/<path to keystore>/keystore.jks
kms.server.ssl.key-store-password=<password for keystore>
kms.server.ssl.key-alias=<SSLCertificateAlias>
```

The KMS will be active after you complete all secure configuration steps and run a `yab update`.

Encrypt Content

KMS encrypts anything defined by the property `kms.encryptkeys`. It is recommended that you do not change the default settings defined for kms.encryptkeys= and that you avoid using references to these properties. These default settings safely limit what values are encrypted, ensuring that you do not encrypt a value that cannot be decrypted and used by another part of the system.

Default passwords and client secrets are initially stored as plain text in the `configuration.properties` file. To encrypt the passwords and client secrets for Tomcat instances and Adaptive UX, update the default settings and run the command `yab kms-encrypt-secrets`.

Note KMS also encrypts content when you run a full system update with `yab update`.

Disable the Key Management Service

To disable the KMS:

1. Edit the KMS properties in the `configuration.properties` file and leave the settings blank.

```
kms.server.ssl.key-store=
kms.server.ssl.keyStoreType=
kms.server.ssl.keyAlias=
kms.server.ssl.key-store-password=
```

2. Run a full system update with `yab update`.

KMS Backup and Recovery

KMS is a critical service. Ensure backups are done regularly and that the backup files are saved off site. Failure to save current backup files could lead to a catastrophic loss of access to your system. See Appendix A, “KMS Backup and Recovery” on page 365, for details.

Database Security

You can secure the connection to your OpenEdge databases and the files on the databases. QAD supports defining OpenEdge database users and table access privileges, and also supports OpenEdge Transparent Data Encryption.

Systems that have multiple databases defined in Database Connection Maintenance (36.6.1) must have a unique parameter file for each database when database security is enabled. The parameter file must include the username and password that were used to secure each database. To determine the necessary username and password, enter:

```
yab <db>.connection.user
yab <db>.connection.password
```

Save the username and password in the parameter file with the following syntax:

```
-U <username> -P <password>
```

The file must:

- Be accessible through the PROPATH or located in the directory specified in Database Directory.
- Not include the `-ld` or `-db` parameters.
- Include the `-trig` parameter, which specifies the location of the trigger file.

Enable Database Security

Database security enforces authentication and authorization by requiring users to enter a username and password to access the OpenEdge database.

Two properties control database security. When set to true, these settings:

- Require users to provide credentials before logging in.
- Prohibit blank users from accessing the database.
- Give the system exclusive responsibility for creating, updating, and deleting database users to match the configuration.

To configure database security, set the following two properties to true in the `configuration.properties` file.

```
db._base.security.authentication=true
db._base.security.user.managed=true
```

Note If you enable database security and are using Audit DB Maintenance (36.12.13.11), you must include the application username and password in the parameter file for the database. See “Manage the Archive Database Server” on page 341 for more information.

Connection User

QAD recommends that you create, at a minimum, a connection user, which is used by the system to connect to the application, create tables and data, and administer the database as a system administrator. The connection user is created and managed by the system and should not reference existing users.

Although it is possible to configure each individual database with a unique connection user, QAD recommends that you define only one connection user as shown in the example. The `db._base` user is propagated to the other databases in the system, which allows you to have the same username and password for the connection user across the system. In addition, there is a known OpenEdge driver limitation when querying multiple databases if they have different passwords.

Important Save OE database username and password values in a separate, secure location. Failure to do so could result in loss of access to the database if the `configuration.properties` file is corrupted.

To create the connection user, define the following properties in the `configuration.properties` file.

```
db._base.connection.user=<username>
db._base.connection.password=<password>
```

Database Users

Optionally, you can set up other database users that are not connection users. The QAD application does not require these users and does not make use of them. These users can be granted access to individual databases by defining a specific database instance. To set up other database users, define the following properties. Replace <INSTANCE> with the database instance and <NAME> with a unique value for each database user.

```
db.INSTANCE.users.NAME.user=<username>
db.INSTANCE.users.NAME.password=<password>
db.INSTANCE.users.NAME.dba=false
```

For existing users, set the following property to false. Do not include this property for new users.

```
db.INSTANCE.users.NAME.managed=false
```

Note All new users are created and managed by the system based on the `db._base.security.user.managed=` setting, which should have been configured as true when enabling database security.

To apply the changes, run a `yab update`.

Database Table Permissions

Before proceeding, ensure that you are familiar with Progress table privilege controls. To enable OpenEdge database table permissions, you must set up a series of rules to control which users, tables, and permissions can be accessed or denied. Be careful with the rules you create to avoid restricting access on too broad a level and do not include the connection user in database table permission settings. Refer to Progress documentation for details on database table security. The following properties define table permissions.

```
db.INSTANCE.table-auth.NAME.includes=
db.INSTANCE.table-auth.NAME.excludes=
db.INSTANCE.table-auth.NAME.users=
db.INSTANCE.table-auth.NAME.permissions=
```

The next example defines a rule that:

- Gives users mfg and test* access to tables with the suffixes _mstr and _det
- Denies access to tables with the prefixes fhd_ and lbs_
- Provides read and create permission for the selected tables

```
db.INSTANCE.table-auth.NAME.includes=*_mstr,*_det
db.INSTANCE.table-auth.NAME.excludes=fhd_*,lbs_*
db.INSTANCE.table-auth.NAME.users=mfg,test*
db.INSTANCE.table-auth.NAME.permissions=can-read,can-create
```

If you are not securing any other part of your system, apply the new settings by entering:

```
yab database-INSTANCE-permissions-update
```

Transparent Data Encryption (Optional)

OpenEdge database Transparent Data Encryption (TDE) provides block-level encryption of data while it is at rest in the file system. TDE provides three important elements:

- Transparency. All data encryption is performed at runtime by the OpenEdge RDBMS without any physical changes to ABL or SQL application code or database design. Application code executes without being aware of whether the database is or is not encrypting its data.
- Configurability. TDE allows you to configure encryption for just the database objects that require it.
- Security. Secure data encryption ensures that once the OpenEdge RDBMS encrypts the data, it cannot be accessed by anyone without proper credentials.

For detailed information, see Progress's OpenEdge TDE documentation.

Encryption Policy

Encryption of database objects is managed through encryption policies. These policies define which objects are encrypted and the encryption cipher for the objects. Policies are stored in your database in a designated Encryption Policy Area and are managed by your system administrator. Object policies use virtual data encryption keys derived from your Database Master Key (DMK) and the specified cipher. The encryption key for each encrypted database object is unique.

Enabling TDE

To enable TDE, the database must have one of the following licenses:

- OpenEdge Enterprise RDBMS and OpenEdge TDE, or alternatively Advanced Enterprise Edition RDBMS, which became available with OE11.5 (for production)
- OpenEdge Development Server (for application deployment)

TDE must be configured by your system administrator. To enable TDE, refer to the official OpenEdge documentation or follow the steps provided here. During this process, you will add an Encryption Policy Area and execute the ENABLEENCRYTPION command.

Important These actions can be done online and offline, but it is recommended that the database be running when you define a new Encryption Policy. While it can be completed with the database offline, the process completes faster with the database running.

Note Do not enable encryption for the compile database, cpldb, or the rcode database, rcddb.

1. Set the umask for the admin user, typically `mfg`, to 002 instead of the default 022. This ensures that the user has write permission to the keystore file <dbname.ks> and allows any new file that gets created to be written by the group. While this step does

not impact TDE configuration, it is required for a successful database restore. If you do not set the umask to 002, a database restore will fail and you will have to change the permissions so the group can write to the <dbname.ks> file.

2 Create a structure (.st) file describing the Encryption Policy Area. The area number must not be in use by another database area definition in the .st file. Enter:

```
encrypt_policy_area.st
e "Encryption Policy Area":90,32,64 . f 1024
e "Encryption Policy Area":90,32,64 .
```

3 Stop the database.

```
yab stop
```

4 Add the Encryption Policy Area to each database where you are enabling TDE. Enter:

```
prostrct add <DBNAME> encrypt_policy_area.st
```

5 Enable encryption and set up a single passphrase. The following command contains the Autostart option, which is required for QAD Adaptive ERP. This step will prompt you for a passphrase for the admin user, which you will need again in step 9.

```
proutil <DBNAME> -C enableencryption -Cipher 2 -Autostart admin
```

This step performs many tasks on your database. Refer to the OpenEdge documentation for more detailed information.

6 Compile the list of table names that you want to encrypt by using the OE data dictionary.

7 Start the databases.

```
yab database-start
```

8 Run the following command for each table to be encrypted. This command must be run once for every table that is to be encrypted.

```
proutil <DBNAME> -C epolicy manage table encrypt PUB.<TABLENAME> -
Passphrase
```

9 Open the `configuration.properties` file and enter the passphrase for the admin user specified during step 5.

```
db._base.keystorepassphrase=<PASSPHRASE>
```

Enable SSL for AppServerDCS

Enabling SSL for AppServers encrypts traffic between clients and the AppServers. The following properties configure security for all AppServers in the environment. Enter them in the `configuration.properties` file.

```
appserver._base.sslenable=1
appserver._base.keyalias=<SSLCertificateAlias>
appserver._base.keyaliaspasswd=<YourSSLKeyAliasPassword>
appserver._base.connectionprotocol=appserverdcs
```

This security functionality can impact system performance. Your system's hardware also can impact performance. To lessen the hit on performance, you can choose to not enable security on individual AppServers, such as the QRA AppServer, as shown in the following example.

```
appserver.qra.sslenable=0
appserver.qra.keyalias=
appserver.qra.keyaliaspasswd=
appserver.qra.connectionprotocol=appserverdc
```

Enable HTTPS for Progress AppServer

Important This section only applies to the users of Adaptive ERP 2024, which supports OpenEdge version 12 (OE12).

Starting from OE12, the classic OpenEdge AppServer is replaced with the Progress Application Server for OpenEdge (PASOE). For more information about Progress Application Server, see Progress Documentation.

Note OE12 provides multiple security improvements. For more information about the security updates, see Progress Documentation.

The PASOE server must be hosted behind the DMZ, preferably in a private LAN that requires a VPN connection for any external connections. Exposing any of the PAS instances on the Internet is not recommended.

To encrypt traffic between clients and the Progress AppServer, enable HTTPS in PAS instances by configuring a JKS keystore with a standard signed certificate. For more information about how to properly configure keystore and certificates, see Progress Documentation.

PASOE supports TLS/SSL transport security. The officially supported version is TLS 1.2. For more information about protocols, ciphers, and certificates, see Progress Documentation.

Example To configure security in the environment, add the following YAB properties:

```
# build/config/configuration.properties or similar configuration recipe file
# Example configuration:

security.keystore.file=[/your/drive/certificates/keystore.jks]
security.keystore.type=JKS
security.keystore.password=[your-passphrase]
security.certificate.alias=[your-wildcard-certificate-alias]

# PASOE with APSV transport
pas._base.connectionprotocol=https
pas._base.catalina.psc.as.https.keystorefile=${security.keystore.file}
pas._base.catalina.psc.as.https.keypass=${security.keystore.password}
pas._base.catalina.psc.as.https.keyalias=${security.certificate.alias}
pas._base.catalina.psc.as.https.storeType=${security.keystore.type}
pas._base.catalina.psc.as.https.compress=off

# PASOE instances with WEB transport
pas._base-classic-ws.connectionprotocol=https
pas._base-classic-ws.catalina.psc.as.https.keystorefile=
${security.keystore.file}
pas._base-classic-ws.catalina.psc.as.https.keypass=
${security.keystore.password}
pas._base-classic-ws.catalina.psc.as.https.keyalias=
${security.certificate.alias}
pas._base-classic-ws.catalina.psc.as.https.storeType=
${security.keystore.type}
pas._base-classic-ws.catalina.psc.as.https.compress=off
```

Note You can define the PASOE settings at the base type level where all PAS instances inherit from.

Securing Data in Transit

Securing data in transit is a security measure for websites that ensures the entire user experience is safe from online threats by encrypting all communication. SSL/TLS encrypts all data in transit shared between a website and a user, protecting the data from unauthorized viewing, tampering, or misuse.

Data in transit is secured by using SSL/TLS in the following components:

- Tomcat servers
- OpenEdge databases

In order to protect and encrypt data, you must have certificates, and your system must be configured to point to those certificates. Configure OpenEdge with the correct certificates for your setup. Refer to Progress documentation for details.

Tomcat Configuration

To configure Tomcat for secure data in transit, a certificate must be placed in a Java keystore.

Important The password for the certificate's private key must match the password for the keystore.

```
tomcat._base.enablesecure=true
tomcat._base.usehttp=false
tomcat._base.keystore=<path to your keystore>/keystore.jks
tomcat._base.keystorepassword=<keystore password>
tomcat._base.usessl=true
tomcat.default.usessl=true
tomcat.eventservice.usessl=true
tomcat.qxtend.usessl=true
tomcat.webui.usessl=true
```

OpenEdge Database Configuration

Configure the following properties for your OpenEdge database. For details on these settings, see the internal `yab help dbserver`.

```
dbserver._base.sslenable=1
dbserver._base.sslkeyalias=<SSLCertificateAlias>
dbserver._base.sslkeyaliaspassword=<YourSSLKeyAliasPassword>


encryptionmethod=ssl
protocolversion=TLSv1.2
ciphersuites=TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256
validateservercert=true
```

If you need to configure a truststore with a certificate, include the following.

```
# @append ;
dbserver._base.jdbc.securityparams=TrustStore=<path to
truststore>;TrustStorePassword=<truststore password>
```

Note When you set up the truststore password, do not use a reference to other properties, such as Tomcat keystore password.

After the system has updated, you can verify your settings by entering `yab config dbserver._base.*` and reviewing the output.

Adaptive UX Support for Encryption

You must configure a setting that enables Adaptive UX to decipher encrypted data. In `configuration.properties`, set:

```
qad-qracore.jdbc.encryption=true
```

After you have updated all relevant properties, review the `configuration.properties` file and then run `yab update`.

Adaptive UX Tomcat Maintenance Mode

During environment creation or a YAB update, Adaptive UX Tomcat server enters maintenance mode, which allows administrators to interact with the system using APIs but blocks users from accessing Adaptive UX sign-in screen. In order for this process to run and complete successfully, the application user that YAB is configured to use must be assigned to a role that allows the use of the system in maintenance mode. The system checks if the role is set in the following locations in the following order:

1. qad-webshell.tomcat.maintenance.mode.role
2. Administrator role in Security Control
3. qadadmin or SuperUser role

During maintenance mode, users are redirected to a screen that displays the message, “Adaptive UX is currently under maintenance and will be back shortly.”

As part of a YAB update, YAB starts Tomcat and then calls APIs to load system data into the database. When all of the data has been processed, YAB starts a refresh of Adaptive UX cache. The completed cache refresh triggers an event in Tomcat to exit maintenance mode.

Maintenance Mode Timeout Setting

In the event that the Tomcat server has not yet exited maintenance mode after a cache refresh and the time defined in the timeout setting is reached, the server will exit maintenance mode and Adaptive UX will be available to users. For most systems, this setting can remain at two hours.

```
qad-webshell.tomcat.maintenance.mode.timeout.seconds=7200 (2 hours)
```

Security with Apache Kafka (Optional)

Apache Kafka is used for building real-time data pipelines and streaming apps. The Adaptive UX uses it in the following components and services:

- Notification Service
- Background Processing

By default when you install Adaptive UX, Kafka connections are not encrypted. It is recommended you obtain certificates and enable security so your data is encrypted.

Enable SSL on the Kafka Server Side

To enable SSL on the server, enter the following settings in the `configuration.properties` file.

```
kafka.default.properties.security.protocol=SSL
kafka.default.properties.ssl.keystore.location=<path to your keystore>/keystore.jks
kafka.default.properties.ssl.keystore.password=<keystore password>
kafka.default.properties.ssl.keystore.type=JKS
kafka.default.properties.ssl.key.password=<key password>
```

Enable SSL on the Kafka Client Side

Multiple components act as Kafka clients, such as Adaptive UX and Nifi. If the server certificate is signed by a trusted CA, no extra properties are required. If the server certificate is self-signed, enter the following settings in the `configuration.properties` file:

```
kafka.default.ssl.client-truststore=<path to your trustscore>
kafka.default.ssl.client-truststore-password=<truststore password>
```

SSL Client Authentication

SSL client authentication allows the server to validate the client's certificate to make sure the client is the one it claims to be. By default, this feature is disabled for Kafka.

To enable this feature, enter the following settings in the `configuration.properties` file.

```
kafka.default.properties.ssl.client.auth=required
```

When enabled, a certificate, stored in a keystore, is required on the client side. Enter the following settings in the `configuration.properties` file.

```
kafka.default.ssl.client-keystore=<path to the client keystore in JKS format>
kafka.default.ssl.client-keystore-password=<the keystore password>
kafka.default.ssl.client-key-password=<the key password>
```

If the certificate is signed by a trusted CA, no extra properties are needed for the server side.

If the certificate is self-signed, configure the server truststore. Enter the following settings in the `configuration.properties` file.

```
kafka.default.properties.ssl.truststore.location=<path to the server truststore>
kafka.default.properties.ssl.truststore.password=<server truststore password>
kafka.default.properties.ssl.truststore.type=JKS
```

Credentials Authentication

Credentials authentication uses Simple Authentication and Security Layer (SASL) to authenticate the Kafka server and client connection with a username and password. To enable credentials authentication, update the security protocol setting in the `configuration.properties` file.

```
kafka.default.properties.security.protocol=SASL_SSL
```

The following simple example uses plain username and password. For the server side, enter these properties in the `configuration.properties` file:

```
kafka.default.username=<Kafka username>
kafka.default.password=<Kafka password>
kafka.default.properties.sasl.enabled.mechanisms=PLAIN
kafka.default.properties.sasl.mechanism.inter.broker.protocol=PLAIN
kafka.default.properties.sasl.mechanism=PLAIN
kafka.default.properties.listener.name.sasl_ssl.plain.sasl.jaas.config=
org.apache.kafka.common.security.plain.PlainLoginModule required username=
"${kafka.default.username}" password="${kafka.default.password}"
user_${kafka.default.username}="${kafka.default.password}";
```

For the client side, enter the following properties in the `configuration.properties` file:

```
kafka.default.sasl.jaas.config=
org.apache.kafka.common.security.plain.PlainLoginModule required username=
"${kafka.default.username}" password="${kafka.default.password}";
```

After you have updated all relevant properties, review the `configuration.properties` file and then run `yab update`.

See Apache Kafka documentation for more information.

Security with Apache Cassandra (Optional)

Apache Cassandra is a key component in the Adaptive UX Action Centers. It is a multi-node, horizontally scalable, columnar database with an embedded SQL-like language. In small- to medium-sized environments, Cassandra is deployed on the same node as the core Adaptive Application infrastructure. In larger environments, it can reside on a dedicated server as part of a larger data lake infrastructure. In very large, multi-site enterprise environments, Cassandra can be deployed as a decentralized cluster with multiple nodes. See the *Adaptive UX Implementation Guide* for detailed information.

Enable SSL

When you install Adaptive UX, Cassandra connections are not encrypted by default. It is recommended that you obtain certificates and enable security to encrypt your data.

To enable SSL on the server side, set the following properties in the `configuration.properties` file.

```
cassandra.default.node.main.client_encryption_options.enabled=true
cassandra.default.node.main.client_encryption_options.keystore=<keystore path>
cassandra.default.node.main.client_encryption_options.keystore_password=<keystore password>
cassandra.default.node.main.client_encryption_options.optional=false
cassandra.default.node.main.client_encryption_options.protocol=TLS
```

If the server certificate is signed by a trusted CA, no extra properties are needed. If the server certificate is self-signed, you must enable SSL on the client side. Enter the following settings in the `configuration.properties` file.

```
cassandra.default.ssl.client-truststore=<truststore location>
cassandra.default.ssl.client-truststore-password=<truststore password>
```

Enable SSL Client Authentication

SSL client authentication allows the server to validate the client's certificate to make sure the client is the one it claims to be. By default, this feature is disabled for Cassandra. To enable SSL client authentication, enter the following setting in the `configuration.properties` file.

```
cassandra.default.node.main.client_encryption_options.require_client_auth=true
```

The client requires a certificate, which is stored in a keystore. Enter the following settings in the `configuration.properties` file.

```
cassandra.default.ssl.client-keystore=<keystore path>
cassandra.default.ssl.client-keystore-password=<keystore password>
cassandra.default.ssl.client-key-password=<key password>
```

If the server-side certificate is signed by a trusted CA, no extra properties are needed. Self-signed certificates require a server truststore. Enter the following settings in the `configuration.properties` file.

```
cassandra.default.node.main.client_encryption_options.truststore=<path to truststore>
cassandra.default.node.main.client_encryption_options.truststore_password=<truststore password>
```

Credential Authentication

Authentication with credentials is independent of SSL and can be enabled independently.

To enable credential authentication, define these settings:

```
cassandra.default.node.main.authenticator=PasswordAuthenticator
cassandra.default.node.main.authorizer=CassandraAuthorizer
cassandra.default.user=<cassandra username>
cassandra.default.password=<cassandra password>
```

After you have updated all relevant properties, review the `configuration.properties` file and then run `yab update`.

See Apache Cassandra documentation for more information.

Security with Apache NiFi

Apache NiFi is designed to automate the flow of data between software systems and is used in background processing in QAD Adaptive ERP. It is important to lock down the port used for NiFi from external traffic, allowing only the system administrator and the local host to have access. To determine the NiFi port, enter:

```
yab config nifi.default.application.nifi.web.http.port
```

The system administrator must secure the port by using an external or internal firewall, such as iptables on Linux systems.

In addition to securing the port, you should enable HTTPS for Nifi. The following sections list the settings you must add to the `configuration.properties` file to turn on and configure the system for HTTPS. Contact QAD Services for assistance.

Enable HTTPS for Nifi

Set the following property to true.

```
nifi.default.secure=true
```

Nifi Server Settings

After you have set the `nifi.default.secure` property to true, define the settings for the Nifi server and its keystore and truststore. You can use the same keystore and certificate you used for Tomcat. See “Java Keystore” on page 39.

```
nifi.default.application.nifi.security.keystore=<keystore>
nifi.default.application.nifi.security.keyPasswd=<key password>
nifi.default.application.nifi.security.keystorePasswd=<keystore password>
nifi.default.application.nifi.security.keystoreType=jks
nifi.default.application.nifi.security.truststore=
${nifi.default.target.dir}/conf/truststore.jks
nifi.default.application.nifi.security.truststorePasswd=<truststore password>
nifi.default.application.nifi.security.truststoreType=jks
```

Self-Signed Certificate for YAB API

QAD recommends using a self-signed certificate that YAB generates and uses for API calls. This certificate gets stored in the Nifi server truststore. If you choose to use a CA-signed certificate, see “CA-Signed Certificate for YAB API” on page 56.

```
nifi.default.client.cert.generated=true
nifi.default.client.cert.generated.cn=admin
nifi.default.client.cert.generated.o=<organization or company name>
nifi.default.client.cert.generated.l=<locality/city>
nifi.default.client.cert.generated.st=<state or province name>
nifi.default.client.cert.generated.c=<country name>
nifi.default.client.cert.generated.duration=2
```

CA-Signed Certificate for YAB API

Skip this section and move on to “Nifi Client Certificate Configuration Settings” on page 56 if you are using a self-signed certificate for YAB to use for API calls.

1. Set the following property to false:

```
nifi.default.client.cert.generated=false
```

2. Place the CA-signed certificate in the server truststore configured in Nifi Server Settings. The three relevant properties are:

```
nifi.default.application.nifi.security.truststore=
${nifi.default.target.dir}/conf/truststore.jks

nifi.default.application.nifi.security.truststorePasswd=<truststore
password>

nifi.default.application.nifi.security.truststoreType=jks
```

Nifi Client Certificate Configuration Settings

Next, for both self-signed and CA-signed certificates, configure the client settings.

```
nifi.default.client.authentication=cert
nifi.default.client.cert.keystore.file=
${nifi.default.target.dir}/conf/keystore.jks
nifi.default.client.cert.keystore.password=<keystore password>
nifi.default.client.cert.keystore.type=jks
nifi.default.client.cert.keystore.alias=nifi-admin-client
nifi.default.client.cert.truststore.file=<keystore>
nifi.default.client.cert.truststore.password=<keystore password>
nifi.default.client.cert.truststore.type=jks
```

Nifi Troubleshooting

In rare instances, background processes may stop unexpectedly. If you cannot resolve the issue from the Background Processing screen in Adaptive UX, check the following logs for error details.

- build/logs/nifi/default/nifi-app.log
- build/logs/nifi/default/nifi-user.log
- build/logs/nifi/default/nifi-bootstrap.log
- servers/tomcat-webui/logs/catalina.out

You can restart Nifi using the command `yab nifi-restart`.

If a restart does not solve the issue, contact QAD Support with the error information from the logs.

Chapter 5

Authentication

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

Overview 58
Describes authentication.

User Authentication 58
Describes how the system validates the identity of a user.

API Authentication 69
Describes the methods that can be used for API authentication.

Smart Card Authentication 70
Describes the properties that must be set to configure smart card authentication.

SAML Single Sign-On 74
Explains the properties necessary to enable single sign-on using Security Assertion Markup Language.

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:

1. Configure Java Keystore.
2. Install DSML Gateway.
3. Review and Update Directory to QAD Database Mappings.
4. Download QAD Adaptive ERP.
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. See “Keystores and Truststores” on page 39 for more information.

Install DSML Gateway

To install and configure 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.opendj.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.opendj.ldap.usessl=. Indicates whether ldap.port points to a port listening for LDAPS (LDAP/SSL) traffic. true or false

   webapp.opendj.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 to trust all certificates blindly, then you must set up a trust store. Not used by default.

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

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

webapp.opendj.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-opendj-update
> yab ldapinstance-opendj-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 opendj instance for a second LDAP service.

```
@extends webapp._base
```

3 Configure the web app settings.

```
webapp.opendj2=
```

Note Do not enter a value for `webapp.opendj2`. This is the configuration syntax for defining a new instance of the webapp type. This example creates “opendj2” webapp. This token can be any valid identifier, but ensure that the type is defined as “opendj.”

webapp.opendj2.context=. The name of the webapp that gets deployed; in this example, `opendj2`.

webapp.opendj2.application=. A parameter required for YAB. Leave as `${packages.opendj-dsml.dir}`

webapp.opendj2.tomcat=. A parameter required for YAB. Leave as `tomcat.default`

webapp.opendj2.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 to trust all certificates blindly, 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 and 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/n/qad.mfgcoreplus/config/user-map.xml`

If you have trouble locating the file, enter:

```
./config/qad.mfgcoreplus/config/user-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 `memberOf`.

Map Element Attributes

Zero or many map elements may be associated with an attribute. If no mapping elements are present, the attribute value is not 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_ctry_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_ctry_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	Email 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
sn	surname	Surname or last name	false	DirectoryString

Attribute Name	Alias	Description	Multiple Values	Syntax
st	stateOrProvinceName	State	false	DirectoryString
street	streetAddress	Street address	false	DirectoryString
uid	userid	Username	false	DirectoryString

Syntax

Attribute Name	Format	Description	Example
Generalized Time	YYYYMMDDHHMMSS[.|,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 Adaptive ERP

Download and open the QAD Adaptive ERP 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 U.S. 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) in QAD Adaptive ERP or LDAP Instances in Adaptive UX to configure LDAP.

1. In QAD Adaptive ERP, 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 checkbox if you are using Active Directory.

2. Click Next in Adaptive ERP or Save in Adaptive UX to save.

Verify LDAP Instance Definition for DSML Gateway Using User Sync

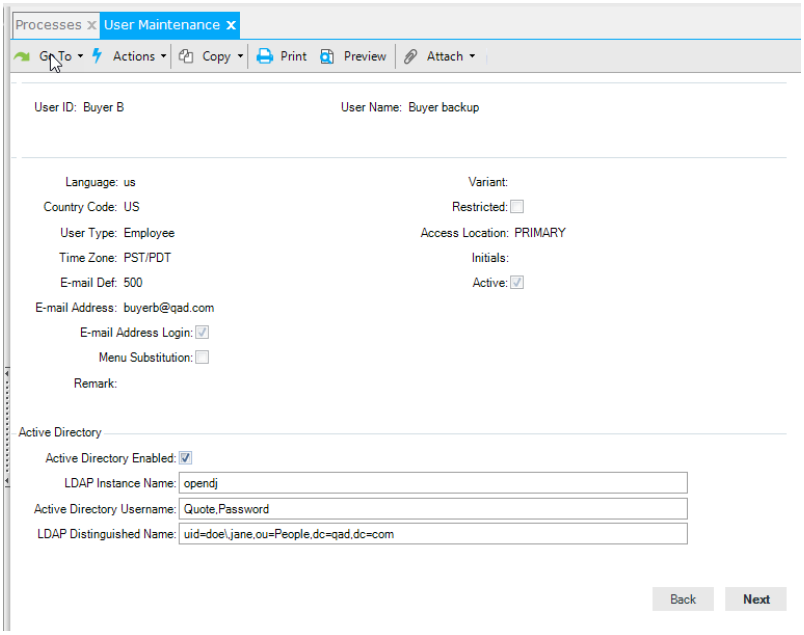
Note You should have your LDAP/Active Directory administrator present when connecting to the authentication server during initial setup and configuration.

QAD Enterprise Edition configures the DSML gateway instance for you. 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. 5.1
User Maintenance



3 Select the Active Directory Enabled checkbox.

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. The LDAP Distinguished Name must be RFC 2253 compliant, which means if an attribute of the distinguished name contains one of the following special characters, that character must be escaped with a backslash (\).

```
",", "+", """, "\", "<", ">" or ";"
```

If you use commas in your usernames, you must escape those commas with a backslash within the LDAP Distinguished Name address. For example, if a username is doe,jane, you would enter `doe\,jane` within the LDAP Distinguished Name address. For example:

```
CN=doe\,jane,OU=Users,OU=Accounts,DC=qad,DC=com
```

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) or the Sync Users action on Users in Adaptive UX to create, update, or deactivate a single user or groups of users. Adaptive Directory User Sync and the Sync Users action perform the same function.

If you are continuing the process in QAD Adaptive ERP, remove the user information from the connection string of the one user you just synced.

- 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.

Fig. 5.2
Active Directory User Sync

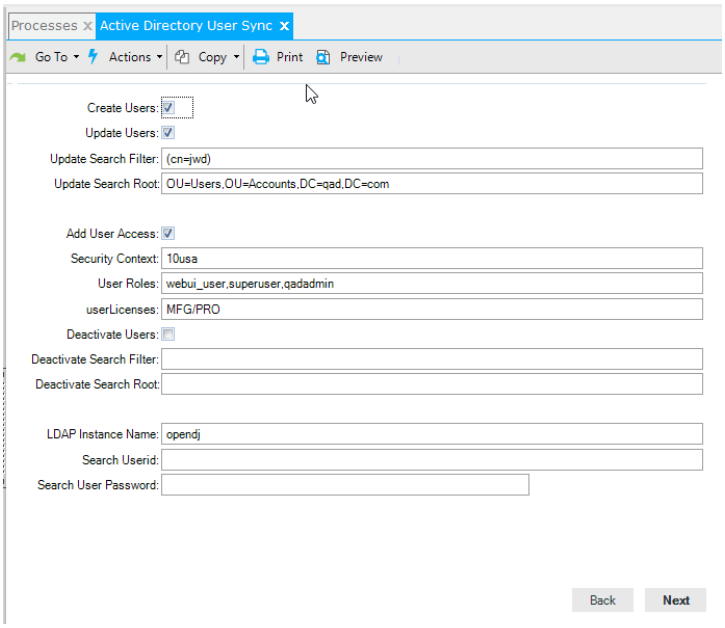
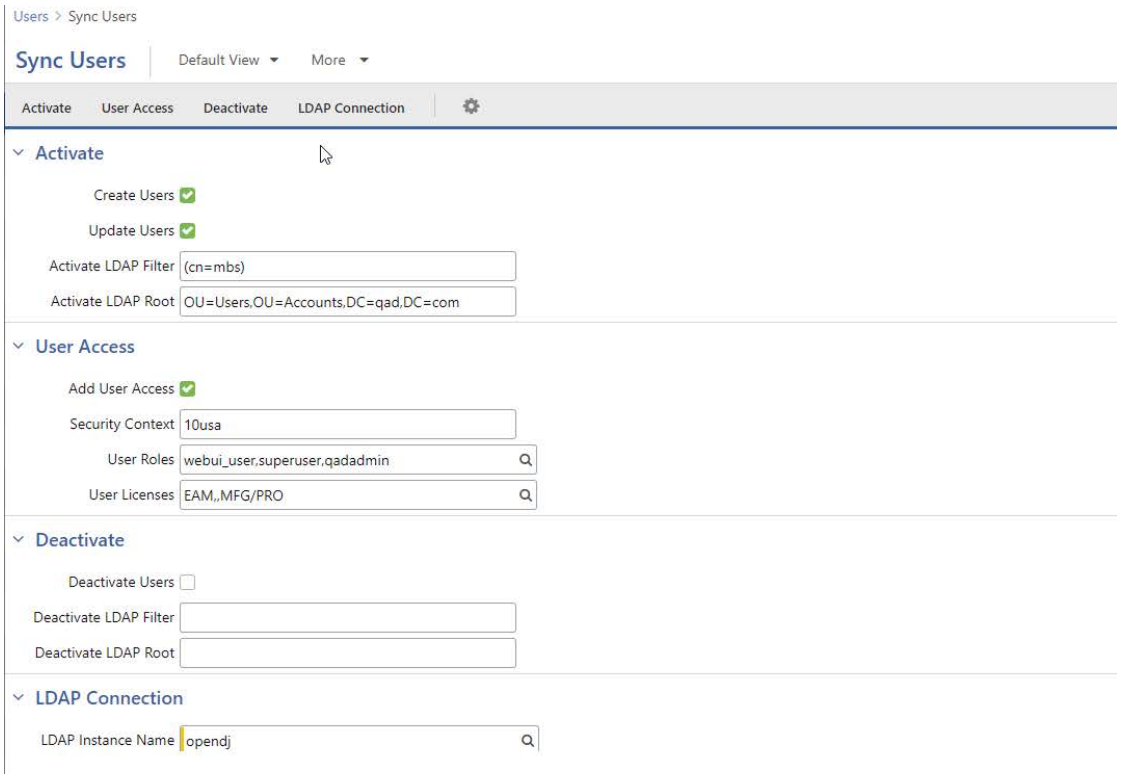


Fig. 5.3
Sync Users



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

Create Users. Selected

Update Users. Selected

Update Search Filter. (memberof=xxx) This field identifies the group being added and is required when Update Users is selected.

Note Use your memberof ID rather than xxx.

Update Search Root. OU=Users,OU=Accounts,DC=qad,DC=com. This field is required when Update Users is selected.

Add User Access. Select this checkbox to update user access to domains and entities in both QAD Adaptive ERP and Adaptive UX.

Security Contexts. Define the domains and related entities to which to assign these users, using the format <domain>/<entity>. Separate multiple domain/entity combinations with a comma and no space. For example, `10USACO/22UK,22UKCO/40BRZ`. You can assign all entities within a domain by specifying only the domain with no associated entity, and you can assign all domains by leaving the Security Context field blank.

User Roles. Specify or select the roles that are being assigned access.

Note In Adaptive UX, select roles one at a time from the lookup. Make the first role you choose the earliest in the alphabet, because upon subsequent launches of the lookup, you only see those roles that alphabetically follow your first selection. For example, if you first choose the required webui_user role, the next time you open the lookup, you would not see any roles that precede webui_user.

User Licenses. Specify or select from the lookup the licenses to assign to these users.

Note In Adaptive UX, select licenses one at a time from the lookup. Make the first license you choose the earliest in the alphabet, because upon subsequent launches of the lookup, you only see those licenses that alphabetically follow your first selection. For example, if you first choose MFG/PRO, the next time you open the lookup, you would not see any licenses that precede MFG/PRO.

Deactivate Users. Do not select this checkbox. Leave subsequent Deactivate-related fields blank.

LDAP Instance Name. The LDAP instance name as specified in LDAP Instance Maintenance

Search UserID. domain\UserID. This field identifies a user that can authenticate against the directory to get access to the directory data. This field is required.

Search User Password. Enter the password for the user specified in Search UserID. This field is required.

2 Click Next.

After processing is complete, you can check output files for more details on the transaction. A system message directs you to the location of the output files. For example,

```
Review these files for results:
/qad/sbox/007/user/mbs/04/env/build/work/client/ldapsync-exceptions.update.xml
/qad/sbox/007/user/mbs/04/env/build/work/client/ldapsync-users.update.xml
```

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.

- OAuth 2 provides a more secure way for REST API clients to authenticate users without sending user credentials with each request. The OAuth 2 Specification requires a client to receive an access token and then pass the token to the resource sever as part of the request.

  The OAuth 2 password grant flow can be used to generate access and refresh tokens for an API user. To use this flow, the client application makes a POST request to the server with the following parameters.

Table 5.1
OAuth 2 Parameters

Property	Description	Example
client_id	The client ID. See “Client ID and Client Secret” for details. Client secret is not required for the POST request.	client_id= f2axx5f024fae0ac4b5460 7f308d1ce5
grant_type	OAuth2 grant type. Use the “password” grant type.	grant_type=password
username	User ID	JonDoe
password	Password	password1234

The POST request looks similar to the following:

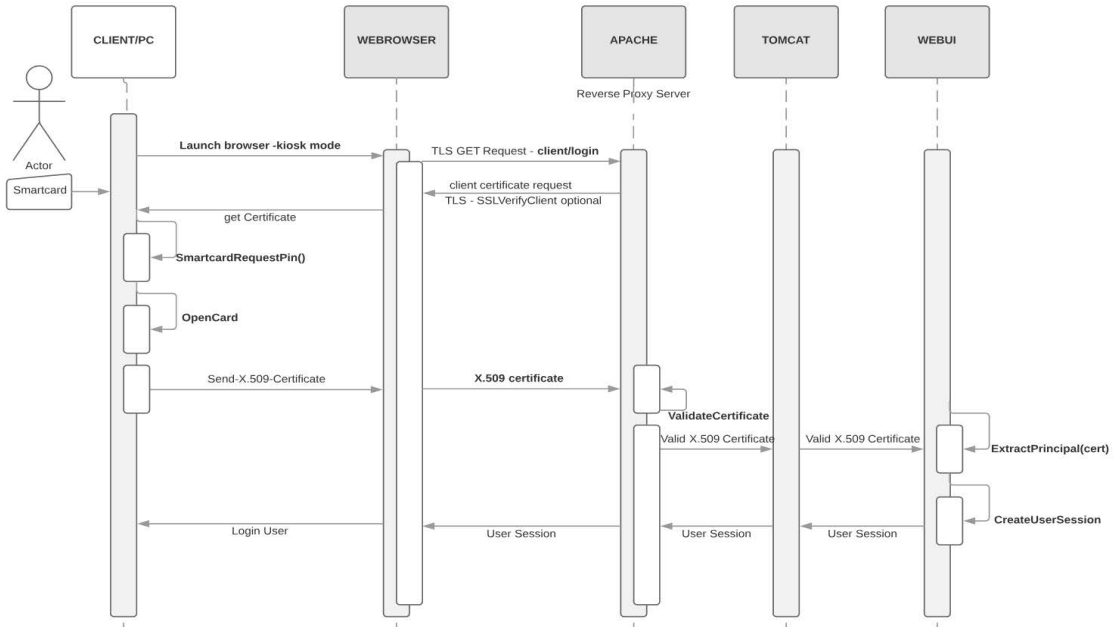
```
POST /clouderp/oauth/token HTTP/1.1
Host: server.company.com
Content-Type: application/x-www-form-urlencoded

client_id=f2axx5f024fae0ac4b54607f308d1ce5&grant_type=password&username=
JonDoe&password=password1234
```

See RFC-6749 for the OAuth 2 Authorization Framework.

Smart Card Authentication

Adaptive UX supports authenticating users through X.509 certificates configured in smart cards. Certificates are exchanged as part of the SSL handshake that occurs during an initial connection. A Certificate Authority (CA) acts as a trusted third party and issues digital certificates that can be added to a smart card to authenticate the smart card user. The Apache reverse proxy server, or Tomcat, validates that the certificate is valid, has not expired, and has not been revoked. Tomcat then sends the certificate to Adaptive UX, which extracts the user principal name and proceeds to sign in the user. This process is illustrated in Figure 5.4.

Fig. 5.4
Smart Card Authentication Sequence Diagram



When using an Apache reverse proxy server, the validation is done by the reverse proxy and the certificate is forwarded to Tomcat. See Chapter 14, “Reverse Proxy for QAD Adaptive ERP,” on page 353 for more information.

The National Institute of Standards and Technology publishes the specifications for cryptographic algorithms and key sizes for personal identity verification, which includes using X.509 certificates. Their document is available at http://dx.doi.org/10.6028/NIST.SP.800-78-4.

Before proceeding, ensure that:

- Your organization supports an internal CA or works with an existing CA to issue certificates that can be deployed to smart cards.
- The certificates issued contain a field with the principal name or email address that can be used to identify the user.

For assistance implementing smart card usage, contact QAD Services.

Define Properties

The only configuration file that you should modify is the `configuration.properties` file, which is used to record changes to the standard configuration defaulted by the system.

To apply your configuration, follow these steps:

1. Define configuration settings in the `configuration.properties` file located in the `build/config/` folder.

   This file contains settings that differ from the base product configuration (`build/config/system`) and initially may be empty. To override a setting, add the property to this file and define the value. If the property is already defined in the file, adjust the value to the desired setting. A sample `configuration.properties` file with SAML SSO examples is available on page 79.

Tomcat Properties

Apache Tomcat is the servlet container that hosts the QAD application. Tomcat can be configured to enable client certificate authentication. Define the properties described in Table 5.2 to configure Tomcat.

Table 5.2
Tomcat Configuration Properties for Smart Card Authentication

Property	Description	Example
tomcat.webui.clientauth	Configures the clientAuth attribute in the Tomcat connector. Possible values are: • false–Default value. No client certificate is required and any client can connect. • true–All clients must provide a certificate. The server does not allow a connection without a certificate. • want–Recommended value. Clients are asked to provide a certificate if available, but the server allows a connection without a certificate. Clients can log in via a certificate when qad-webshell.certificate.authentication.enabled=true.	tomcat.webui.clientauth=want
tomcat.webui.truststore	The trust store file to use to validate client certificates. If no value is set, the default file $JAVA_HOME/jre/lib/security/cacerts is used.	tomcat.webui.truststore=/path/truststorefile.jks
tomcat.webui.truststorepass	The password to access the trust store	tomcat.webui.truststore=passphrase

Certificate Configuration Properties

In addition to enabling Tomcat, you must enable clients to be authenticated with certificates. Client authentication allows the server to validate the end user who is connecting to the system through the use of a certificate. A client digital certificate is usually a file protected with a password and loaded into a client application. This authentication step can disable anonymous users from reaching the service.

Define the properties described in Table 5.3 to complete this step.

Table 5.3
Certificate Configuration Properties for Smart Card Authentication

Property	Description	Example
qad-webshell.certificate.authentication.enabled	Enables certificate-based authentication. Default value: false.	qad-webshell.certificate.authentication.enabled=true
qad-webshell.certificate.subject-principal-regex	The regular expression to extract the principal from the certificate, where the principal is a string that identifies the user. Default value: emailAddress=(.*?)(?:,|$). The default setting attempts to retrieve the email address from the certificate. You must adjust this setting if your certificate is configured differently. Other supported value: • User ID from User Maintenance	qad-webshell.certificate.subject-principal-regex=emailAddress=customer@qad.com. qad-webshell.certificate.subject-principal-regex=userID=qad
qad-webshell.certificate.proxy.server	Required when using an Apache reverse proxy. The server name of the Apache reverse proxy host.	reverse-proxy.qad.com
qad-webshell.certificate.jwt.clientId	The client ID. See “Client ID and Client Secret”	qad-webshell.certificate.jwt.clientId=ad75fe81eb6462b53e14846be83efeee
qad-webshell.certificate.jwt.clientSecret	The client secret. See “Client ID and Client Secret”	qad-webshell.certificate.jwt.clientSecret=4lSkeOGuYm/rz57L+TOGWjNU5+Ls2ibgVtZg7dile2M=
qad-webshell.certificate.jwt.expires.seconds	Optional. The token’s expiration, in seconds. Default value is 300.	qad-webshell.certificate.jwt.expires.seconds=300

2 Update your environment. To run only the specific steps related to smart card authentication, enter:

```
> yab webapp-webshell-config-content-update tomcat-webui-update tomcat-webui-stop tomcat-webui-start
```

To update your entire environment, enter:

```
> yab update
```

Apache Proxy Configuration

When using an Apache server configured as a reverse proxy to validate and extract the client certificate, you must add the Apache reverse proxy configuration as root and restart the httpd service. See Apache documentation for setup instructions.

After the reverse proxy configuration is defined, create a location for a certificate client authentication entry point. This location ensures the client certificate is requested when accessing the main smart card authentication entry point.

```
<Location alias/[environment-alias]/certificate/login>
    RequestHeader set SSL_CLIENT_CERT ""
    RequestHeader set SSL_CLIENT_VERIFY ""
    RequestHeader set SSL_CLIENT_CERT "%{SSL_CLIENT_CERT}s"
    RequestHeader set SSL_CLIENT_VERIFY "%{SSL_CLIENT_VERIFY}s"
    RequestHeader add X-Forwarded-Scheme https
    SSLVerifyClient
    SSLVerifyDepth 5
    SSLOptions +ExportCertData
</Location>
```

Note `[environment-alias]` is the proxy alias location for the actual configured environment.

Refer to Apache documentation for appropriate `SSLVerifyDepth` values, which depend on the type of certificates and length of chained SSL certificates.

In addition, ensure that a CA is configured to validate the provided client certificates. This directive is global for SSL setup and cannot be specified on a <Location> directive. The Apache configuration has the following directive that points to a CA certificate file:

```
# Certificate Authority (CA):
SSLCACertificateFile "/etc/pki/tls/certs/corp-ca.crt"
```

Refer to Apache documentation for complete SSL Apache configuration details.

SAML Single Sign-On

QAD supports single sign-on using Security Assertion Markup Language 2.0 (SAML). This section explains the properties that must be defined to enable SAML SSO.

Required Properties for SAML SSO

SAML SSO is configured using property settings in the following areas:

- Service Provider (SP): An external vendor providing a service. An application software service provider in a service-oriented architecture. In this context, the service provider is a QAD application such as Enterprise Edition.
- Identity Provider (IdP): A service that manages user authentication. OneLogin and OKTA are examples of IdPs.
- Reverse Proxy (RP): A type of proxy server that retrieves resources on behalf of a client from one or more servers. These resources are then returned to the client as if they originated from the Web server itself.
- JSON Web Token (JWT): A method of ensuring data sent between two parties was created by an authentic source and has not been changed. Data is encoded as a JSON object.

The only configuration file that you should modify is the `configuration.properties` file, which is used to record changes to the standard configuration defaulted by the system.

To apply your configuration, follow these steps:

1. Define your configuration settings in the `configuration.properties` file located in the `build/config/` folder.

   This file only contains settings that differ from the base product configuration (`build/config/system`) and initially may be empty. To override a setting, add the property to this file and define the value. If the property is already defined in the file, you can adjust the value. You can view a `configuration.properties` file with SAML SSO examples on page 79.

Define the properties described in Table 5.4 to enable and configure SAML SSO.

Table 5.4
SAML SSO Configuration Properties

Property	Description	Example
qad-webshell.saml.enabled	Set to true to enable SAML SSO functionality. If the property is missing, has an empty string, or has any value other than true, SAML SSO is disabled.	qad-webshell.saml.enabled=true
qad-webshell.saml.idp.maxAuthenticationAge.seconds	The amount of time, in seconds, that the system allows users to remain signed in with each single sign-on. This optional setting defaults to 259200 seconds (72 hours).	qad-webshell.saml.idp.maxAuthenticationAge.seconds=259200
qad-webshell.saml.sp	An arbitrary string that serves as the SP entity ID. QAD always sets this as the URL to the service provider. Value must be unique within an IdP.	qad-webshell.saml.sp= https://customer.qad.com/clouderp
qad-webshell.saml.idp.0.alias	The alias for an IdP that is used as a request parameter for the SSO process. See “Identity Provider Properties”	qad-webshell.saml.idp.0.alias= onelogin
qad-webshell.saml.idp.0.metadata.url	Defines the URL from which IdP metadata is taken. Each IdP has a unique metadata URL for each SP within it. See “Types of Metadata URL Properties”	qad-webshell.saml.idp.0.metadata.url= https://app.onelogin.com/saml/metadata/958214
qad-webshell.saml.idp.0.logout.url	Defines the link to the page to which users are redirected if they select Sign Out. URLs can be relative or fully qualified. Relative URLs must start with a forward slash.	qad-webshell.saml.idp.0.logout.url= https://customer.onelogin.com/portal
qad-webshell.saml.jwt.clientId	The client ID. See “Client ID and Client Secret”	qad-webshell.saml.jwt.clientId= avcf0aerb2b32dbc3l14c390502c5900

Property	Description	Example
qad-webshell.saml.jwt.clientSecret	The client secret. See “Client ID and Client Secret”	qad-webshell.saml.jwt.clientSecret= zsSMtrHLMFDxG3dhEc3lTtXIyGvPB EhPn46wraCPLP8=
qad-webshell.saml.jwt.expires.seconds	The token’s expiration, in seconds. Default value is 300.	qad-webshell.saml.jwt.expires=300

2 Update your environment. To run only the specific steps related to SAML SSO, enter:

```
> yab webapp-webshell-config-content-update tomcat-webui-stop tomcat-webui-start
```

To update your entire environment, enter:

```
> yab update
```

Types of Metadata URL Properties

URLs where metadata is stored can be set using three formats:

1 **Classpath URL**. Metadata is picked up from a file placed on the application’s classpath directory in `[tomcat_directory]/webapps/[app_directory]/WEB-INF/classes`. The URL must start with `classpath:` followed by the file name where the IdP metadata is located. The configuration may look like:
`qad-webshell.saml.idp.0.metadata.url=classpath:onelogin_metadata_769206.xml`

2 **File URL**. Metadata is picked up from a file placed somewhere on the file system. The URL must start with `file:` followed by the file system address of the file where the IdP metadata is located. The configuration may look like:
`qad-webshell.saml.idp.0.metadata.url=file:/qad/local/sandbox/team/webui-sm2/config/onelogin_metadata_769206.xml`

3 **HTTPS URL**. Metadata is downloaded via HTTP from a URL. The URL must start with `https` and represent an internet address where the IdP metadata is located. The configuration may look like:
`qad-webshell.saml.idp.0.metadata.url=https://app.onelogin.com/saml/metadata/769206`

Important It is not recommended to use HTTPS URL metadata downloading due to the possibility of a Man in the Middle attack.

While these URL types can be mixed in one configuration set, it is not recommended.

Identity Provider Properties

At least one set of IdP properties should be set for `alias`, `metadata.url`, and `logout.url`. The set with an index value of 0 is considered the default and is used if no IdP parameter is used with the /saml/login URL.

You can create additional groups of the `alias`, `metadata.url`, and `logout.url` properties by changing their index numbers. By default, you can set four sets of indices, from 0-3. For example:

```
qad-webshell.saml.idp.1.alias=<IdP alias>
qad-webshell.saml.idp.1.metadata.url=<IdP metadata URL>
qad-webshell.saml.idp.1.logout.url=<URL to logout page>
```

Client ID and Client Secret

The client ID and client secret settings can be created in either QAD Adaptive ERP or Adaptive UX.

Note QAD highly recommends that you generate a new client ID for each application that is calling an API so you can identify the individual applications. For example, you should have a separate client ID and secret for SAML SSO, smart card authentication, and OAuth2. Only use the new IDs for their defined purposes.

1. Go to Client ID Maintenance (36.3.12) in QAD Adaptive ERP or Client IDs in the QAD Adaptive UX. In Adaptive UX, select New.
2. Select Generate to create a new client ID and client secret.

Fig. 5.5
Client ID Maintenance (QAD Adaptive ERP)

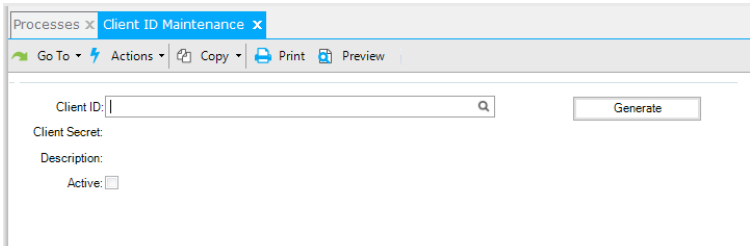
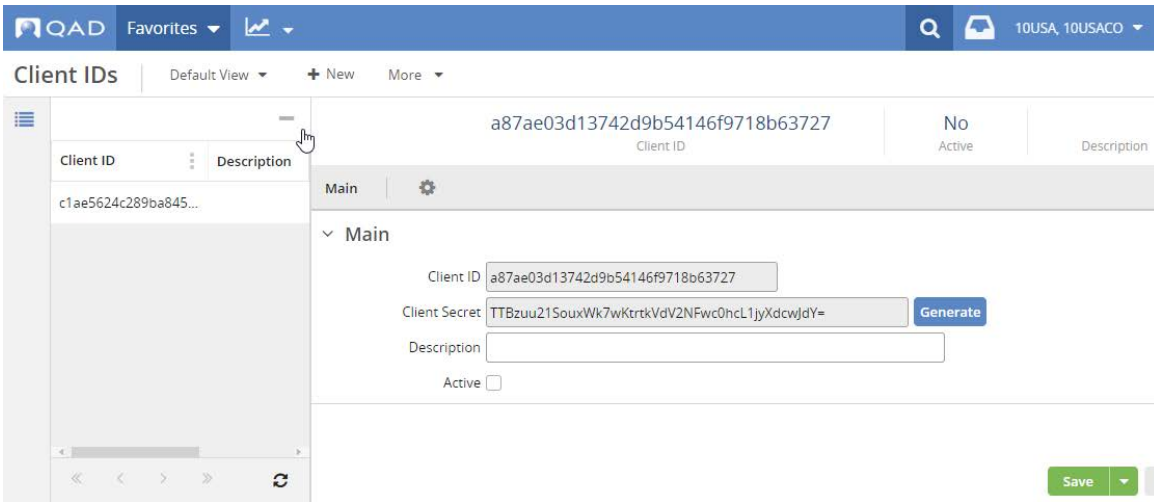
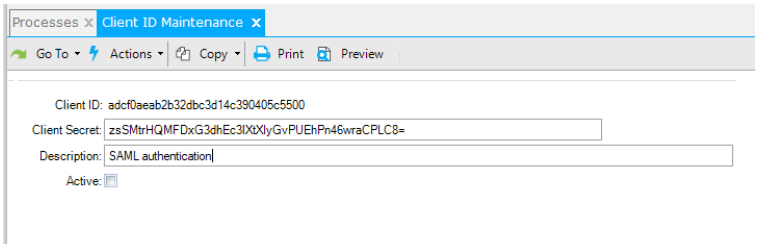


Fig. 5.6
Client IDs (QAD Adaptive UX)



3. Enter a description of the generated client ID and select the Active checkbox. Click Next in Adaptive ERP or Save in Adaptive UX to save.

Fig. 5.7
New Client ID and Secret



4 Copy the Client ID value and paste it into the `build/config/configuration.properties` file for the Client ID property.

5 Copy the Client Secret value and paste it into the `build/config/configuration.properties` file for the Client Secret property.

Note The Client Secret value should be kept confidential. It should not be available outside of the `configuration.properties` file, which itself should have appropriate OS permissions set. If at any time this value is compromised, generate a new secret and update your `configuration.properties` file.

SAML-specific Logout Behavior

When SAML is enabled and properly configured, users who have logged in using SAML are redirected to an IdP-specific logout URL when they select Sign Out. The URL is configured with the `qad-webshell.saml.idp.[index].logout.url` property.

Note All other login and logout cases use the `qad-webshell.login.url` and are not SAML specific. If this property is not defined, the default value is:

```
qad-webshell.login.url=/resources/login.jsp
```

SAML Endpoints

SAML functionality can be used with the following endpoints.

Table 5.5 SAML Endpoints

Endpoint	Description
/saml/login	SSO with IdP configured with qad-webshell.saml.idp.0.... properties.
/saml/login?idp=your_alias	SSO with IdP configured with qad-webshell.saml.idp.[index].alias=your_alias and the related properties of qad-webshell.saml.idp.[index].metadata.url and qad-webshell.saml.idp.[index].logout.url.
/saml/metadata	Generation service provider metadata XML file.

/saml/metadata File

The `/saml/metadata` file contains information, such as service provider ID (entity ID) and SSO endpoints (AssertionConsumerService), that can be used to set property values in the `configuration.properties` file. It can be useful to have the `/saml/metadata` file available while you are entering data in the `configuration.properties` file. Following is a sample `/saml/metadata` file.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ID=
    "https___customer.qad.com_clouderp_devl" entityID=
    "https://customer.qad.com/clouderp/devl">
    <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        Location="https://customer.qad.com:443/qad-central/saml/SingleLogout"/>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
        Redirect" Location="https://customer.qad.com:443/qad-central/saml/SingleLogout"/>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
        format:emailAddress</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
        format:transient</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
        format:persistent</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
        format:unspecified</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
        format:X509SubjectName</md:NameIDFormat>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
        POST" Location="https://customer.qad.com:443/qad-central/saml/SSO" index="0"
        isDefault="true"/>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
        Artifact" Location="https://customer.qad.com:443/qad-central/saml/SSO" index="1"/>
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Sample build/config/configuration.properties File

```
qad-webshell.login.url=/resources/login.jsp

# SAML SP configuration
qad-webshell.saml.sp=https://customer.qad.com/clouderp

# SAML OneLogin IdP configuration
qad-webshell.saml.idp.0.alias=onelogin
qad-webshell.saml.idp.0.metadata.url=https://app.onelogin.com/saml/metadata/958214
qad-webshell.saml.idp.0.logout.url=https://customer.onelogin.com/portal

# SAML OKTA IdP configuration
qad-webshell.saml.idp.1.alias=okta
qad-webshell.saml.idp.1.metadata.url=
https://customer.oktapreview.com/app/jslew4acl9jle2sWMuN8e5/sso/saml/metadata
qad-webshell.saml.idp.1.logout.url=https://customer.oktapreview.com/app/UserHome

# SAML JWT configuration
qad-webshell.saml.jwt.clientId=avcf0aerb2b32dbc3l14c390502c5900
qad-webshell.saml.jwt.clientSecret=zsSMtrHLMFDxG3dhEc3lTtXIyGvPBEhPn46wraCPLP8=
qad-webshell.saml.jwt.expires.seconds=300
```

Single Sign-On to QAD Adaptive ERP

SAML SSO is supported in QAD Adaptive ERP but is dependent on the SAML functionality within Adaptive UX. Adaptive UX can launch QAD Adaptive ERP screens and pass a one-time token to automate the login process to QAD Adaptive ERP. To

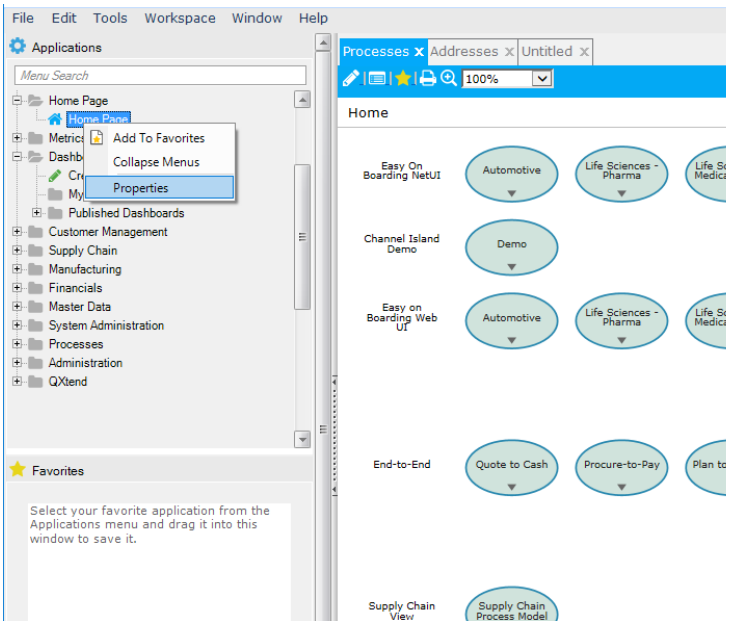
enable single sign-on for the QAD Adaptive ERP, create a shortcut on your desktop and enter a URL that contains the Adaptive UX base URL combined with the QAD Adaptive ERP URL for the menu item key of the .NET screen you want to land on. The following steps describe one way to create and populate the shortcut.

1. Open Notepad and save the file with a URL extension. For example, `QADNET.url`
2. In the Notepad file, enter the following:

   ```
   [InternetShortcut]
   URL=https://<server name>/<app name>/link/netui/menu?menuitem-key=<menu item key>
   ```

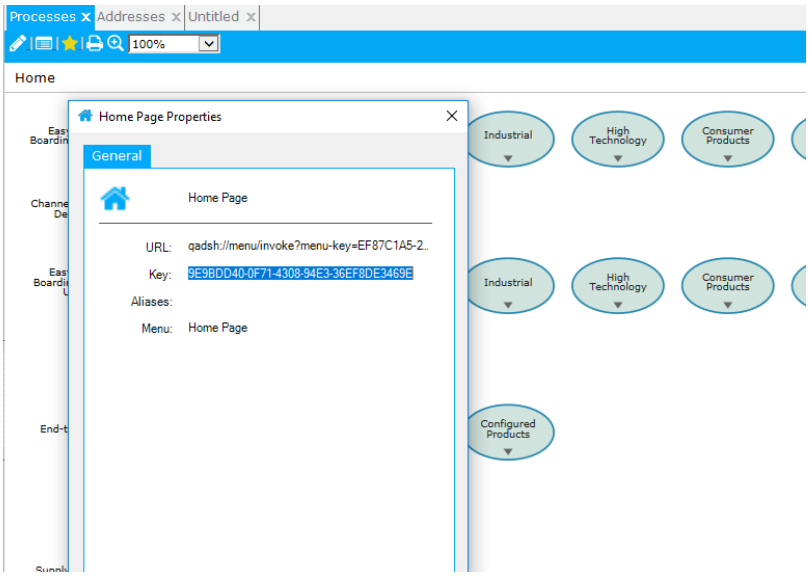
3. In the URL, replace `//<server name>/<app name>` with the base URL for your Adaptive UX instance. The app name is likely to be either `clouderp` or `qad-central`; for example, `//server.qad.com/qad-central`.
4. Determine the page on which you want to land in the QAD Adaptive ERP. In .NET, right-click on that page in the Applications menu and select Properties.

Fig. 5.8
Properties



5. In the Properties dialog box, highlight and copy the Key value text. For many menu items, this value is the menu item number, such as 1.4.1. For others, including the Home Page and all Enterprise Asset Management screens, the value is a string of letters and numbers.

Fig. 5.9
Key Value



6 In the Notepad file, replace `<menu item key>` with the Key text you copied in the Properties dialog box.

7 Your file should look similar to:

```
[InternetShortcut]
URL=https://server.qad.com/clouderp/link/netui/menu?menuitem-key=1.4.1
```

8 Save the file. The shortcut is complete.

SAML SSO Troubleshooting

To enable SAML-related logs of DEBUG level, add the following line to the `logback.xml` file between the `<configuration></configuration>` elements.

```
<logger name="org.springframework.security.saml" level="debug"/>
```

The `logback.xml` file can be modified during runtime and the changes are applied within 10 seconds.

Tomcat Fails During Startup

1 An IdP is not configured. Catalina.out contains the following error:

```
ERROR com.qad.webshell.security.authentication.saml.SamlProperties: There must be at least one Identity Provider (IDP)
```

Tomcat does not start and throws the exception:

```
java.lang.IllegalArgumentException: There must be at least one Identity Provider (IDP)
```

Solution: Configure at least one IdP in `configuration.properties`.

2 The `qad-webshell.saml.idp.[index].alias` property is not defined. Catalina.out contains the following error:

```
ERROR com.qad.webshell.security.authentication.saml.IdentityProviderProperties: 'alias' field must not be empty
```

Tomcat does not start and throws the exception:

```
java.lang.IllegalArgumentException: 'alias' field must not be empty
```

Solution: Define the `qad-webshell.saml.idp.[index].alias` property in `configuration.properties`.

3 The `qad-webshell.saml.idp.[index].metadata.url` property is not defined. Catalina.out contains the following error:

```
ERROR com.qad.webshell.security.authentication.saml.IdentityProviderProperties:
'metadataUrl' field must not be empty
```

Tomcat does not start and throws the exception:

```
java.lang.IllegalArgumentException: 'metadataUrl' field must not be empty
```

Solution: Define the `qad-webshell.saml.idp.[index].metadata.url` property in `configuration.properties`.

4 The `qad-webshell.saml.idp.[index].logout.url` property is not defined. Catalina.out contains the following error:

```
ERROR com.qad.webshell.security.authentication.saml.IdentityProviderProperties:
'logoutUrl' field must not be empty
```

Tomcat does not start and throws the exception:

```
java.lang.IllegalArgumentException: 'logoutUrl' field must not be empty
```

Solution: Define the `qad-webshell.saml.idp.[index].logout.url` property in `configuration.properties`.

5 The `qad-webshell.saml.idp.[index].metadata.url` property is invalid. Catalina.out contains an error similar to the following:

```
ERROR org.opensaml.saml2.metadata.provider.AbstractReloadingMetadataProvider: Error
occurred while attempting to refresh metadata from
'https://app.onelogin.com/saml/metadata/787727xxx'
org.opensaml.saml2.metadata.provider.MetadataProviderException: Non-ok status code 404
returned from remote metadata source https://app.onelogin.com/saml/metadata/787727xxx
```

Tomcat does not start and throws the exception:

```
org.opensaml.saml2.metadata.provider.MetadataProviderException: Non-ok status code 404
returned from remote metadata source https://app.onelogin.com/saml/metadata/787727xxx
```

Solution: Enter a valid URL from which metadata can be taken for the `qad-webshell.saml.idp.[index].metadata.url` property in `configuration.properties`.

Access Token Does Not Pass Validation

When client ID or client secret values are not properly configured, an error occurs during authentication and the following message appears on Adaptive UX sign-in screen:

```
Unable to sign in: access token did not pass validation.
```

The JWT-related values of client ID or client secret did not pass Business Layer validation because of inconsistencies between the values stored on the Business Layer and the JWT-related properties stored on Tomcat.

Solution: Ensure the properties for `qad-webshell.saml.jwt.cientid` and `qad-webshell.saml.jwt.clientSecret` in `configuration.properties` are identical to the values configured in Client ID Maintenance (36.3.12) for the SAML SSO-specific Client ID and Client Secret values.

Error Validating SAML Message

When an error occurs during SAML validation, the following message appears on Adaptive UX sign-in screen:

```
Unauthorized. Authentication Failed: Error validating SAML message.
```

Two known issues can cause this error.

- Destination Endpoint Does Not Match the Recipient Endpoint
- Local Entity is Not the Intended Audience

Destination Endpoint Does Not Match the Recipient Endpoint

The destination and recipient endpoints could be incorrectly defined in two different ways. The endpoints may not match because a direct server URL is being used or because the IdP SSO request URL differs from what has been defined.

1. The SAML SSO API (saml/login) must match the property defined for `qad-webshell.saml.rp.url`. If the SAML SSO API is invoked using a direct server URL and the `qad-webshell.saml.rp.url` property refers to the URL of a reverse proxy, the validation fails.
2. The IdP SSO request URL must match the property defined for `qad-webshell.saml.rp.url`. An error occurs when the RP server setting in `httpd.conf` on the Apache server differs from the URL configured for `qad-webshell.saml.rp.url`.

Solution: Ensure the proxy URL defined for `qad-webshell.saml.rp.url` is used for the SAML SSO API and the IdP SSO request URL.

Local Entity is Not the Intended Audience

The Audience value of the IdP differs from the SP entity ID defined for `qad-webshell.saml.sp` in `configuration.properties`.

Solution: Ensure the Audience field value in the IdP configuration is the same as the `qad-webshell.saml.sp` property in the `configuration.properties` file.

Chapter 6

Users and Roles

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

Overview 86
Describes role-based access control and its purpose.

Set Up Roles 88
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.

Set Up Users 104
Illustrates how to set up users, define the different types of users, and specify access to domains and entities.

Define Role Membership 119
Describes how to define an association between a system role and a user, and to indicate which role is the user's default role.

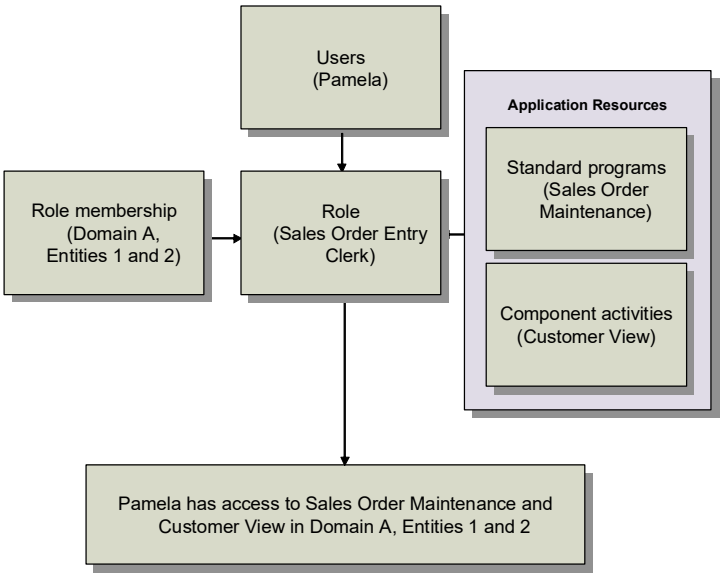
Role and User Audit Reports 123
Explains how to generate audit trail reports and review changes made to roles, role permissions, etc.

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

Fig. 6.1
Users and Roles



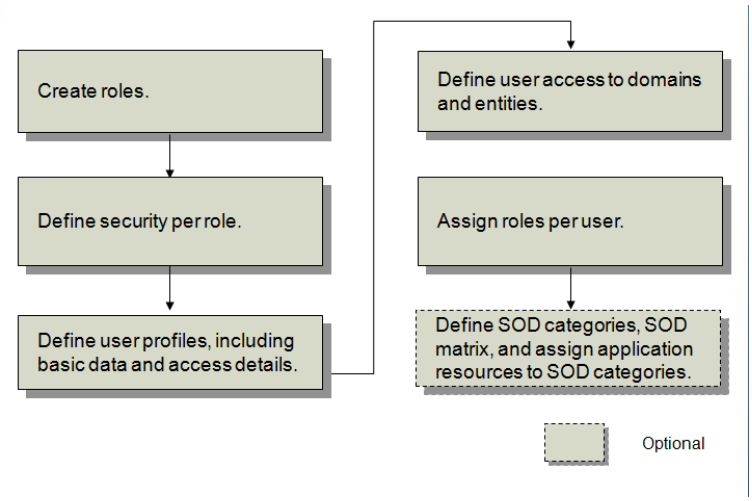
Role and User Definition Process Workflow

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.

To set up and configure users and roles in your system, use the programs in the System Security Menu in QAD Adaptive ERP and the Roles and Users screens in Adaptive UX. Figure 6.2 shows the user and role setup process workflow.

Note You must assign users to roles in both QAD Adaptive ERP and Adaptive UX in order for users to access both interfaces. Assigning users to roles in Adaptive ERP does not automatically grant a user access to Adaptive UX.

Fig. 6.2
Roles and Users Setup Flow



Note The overall flow used to set up users and roles is consistent between QAD Adaptive ERP and Adaptive UX. The following workflow contains information specific to QAD Adaptive ERP. For Web UI-specific information, see “Role and User Workflow in Adaptive UX” on page 128.

1. Create roles in Role Create (36.3.6.1) in Adaptive ERP or Roles in Adaptive UX. All system users must be assigned to a role before they can access the system. For details, see “Set Up Roles” on page 88.

2. 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 101.

3. Create system users in User Maintenance (36.3.1) in Adaptive ERP or Users in Adaptive UX, 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 104.

4. 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 115.

5. 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 119.

6. If you are implementing EAM, you must complete additional setup in QAD Adaptive ERP, such as downloading the users to EAM that you created in step 3 and linking the EAM administrative user to a site. See the *QAD Enterprise Asset Management User Guide* for detailed information.

7. 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 9, “Segregation of Duties in Adaptive ERP,” on page 199.

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 119.

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 8, “QAD Adaptive ERP Security,” on page 173.
- 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 Adaptive Applications User Guide*.

Note The Process Maps display on the menu in QAD Adaptive ERP, 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, users are 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 roles 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.

Adaptive UX 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 cannot update the default roles but you can assign users to them. You can review the default roles' associated permissions on the Role Menus and Role Permission screens 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 Adaptive UX role based on a default or existing role, see "Role Menus" on page 129 for information on copying menu items and setting permissions.

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

Table 6.1
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*.
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.

Secured Item	Description
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 Adaptive 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 106.
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 in Adaptive ERP. Table 6.2 lists these roles and their functions.

Table 6.2
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 email 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 email 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 email 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 email 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 105.

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.
- QAD Adaptive ERP 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 6.3, Jane's roles grant her entry to all the levels she is authorized to access.

Fig. 6.3
Using Roles to Give Access

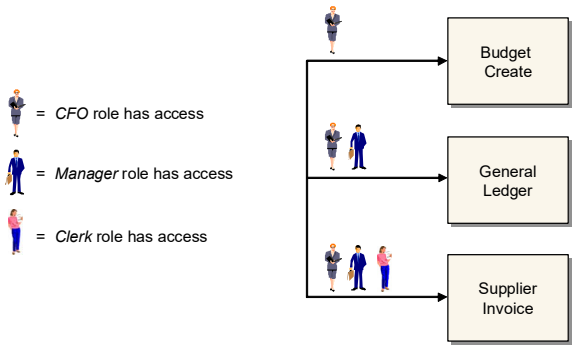


Table 6.3 shows how the system administrator assigns users to each role.

Table 6.3
Sample Role Setup

Role	User
Clerk	Sara, Don, Jane
Manager	Don, Jane
CFO	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 QAD Adaptive ERP, users can also create their own custom menu display under Favorites.

Define Roles

In QAD Adaptive ERP, use Role Create (36.3.6.1) and in Adaptive UX, use Roles to define roles in your system. You should define as many roles as required in order to model your business processes in the system. In Adaptive ERP, use Role Modify

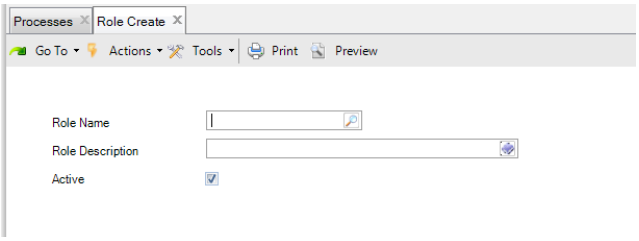
(36.3.6.2) to perform maintenance on existing roles defined in your system, and Role View (36.3.6.3) to view roles. These activities can all be done in Adaptive UX from the Roles screen.

Adaptive UX roles can be set up and maintained in both Adaptive ERP and Adaptive UX. Roles created in Adaptive UX are immediately accessible in Adaptive ERP. If you create roles in the QAD Adaptive ERP meant for Adaptive UX, the roles' permissions should be configured using role menus in Adaptive UX. See "Menus" on page 129.

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

Create a New Adaptive ERP Role

Fig. 6.4
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 Adaptive 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.

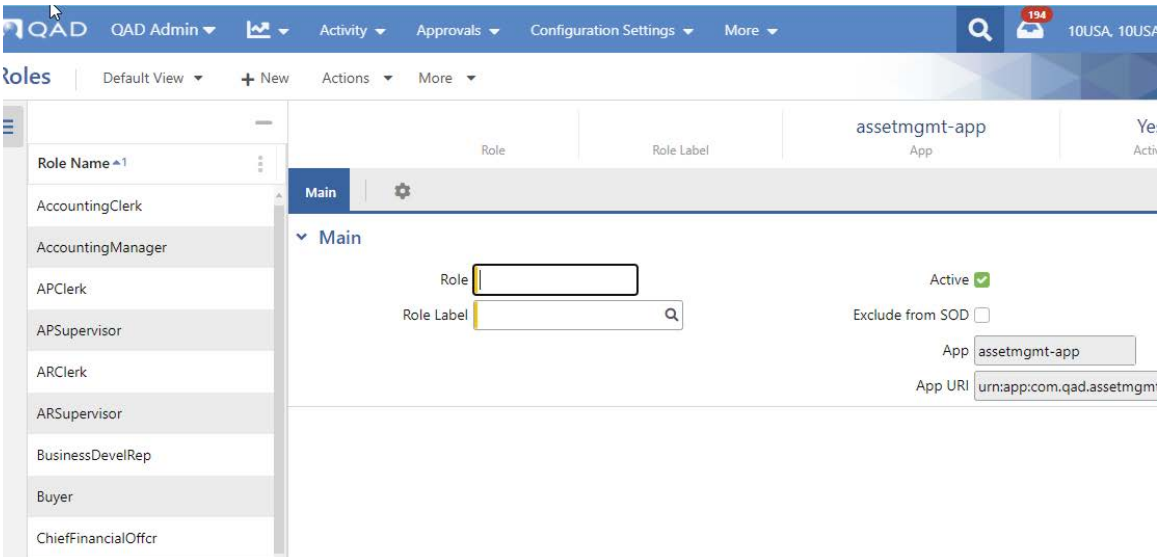
Active. Indicate if this is an active record.

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.

Create a New Adaptive UX Role

1 Select New.

Fig. 6.5
New Role



2 Enter a role name in the Role field.

3 Enter a label for the role in the Role Label field. The label name displays as an option in the roles and favorites drop-down menu for users assigned to the new role. You can select a string code from the lookup, which allows the role label to be translated.

4 Leave the Active checkbox selected to make the role active in the system upon save.

5 Select the Exclude from SOD checkbox if this role should be excluded from segregation of duties validation checking. This option is useful for roles applied to technical superuser accounts used to query the database and perform actions when external systems integrate with QAD Financials.

Important Segregation of duties role exclusion is the highest level of segregation of duties policy exception and should be used carefully.

6 The App and App URI fields are provided for informational purposes. The App field displays the app to which this role belongs. For QAD system roles, the role is part of the associated app. For example, the Sales Marketing Ops role belongs to the Customer Relationship Management app (custrelmgmt-app) and the Maintenance Planner role belongs to the Asset Management app (assetmgmt-app). New roles are always created as part of the Configuration Data app and can be exported and imported into different environments without going through the Software Development Life Cycle process. See the *QAD Enterprise Platform Developers Guide* for detailed information on Configuration Data.

7 Select Save.

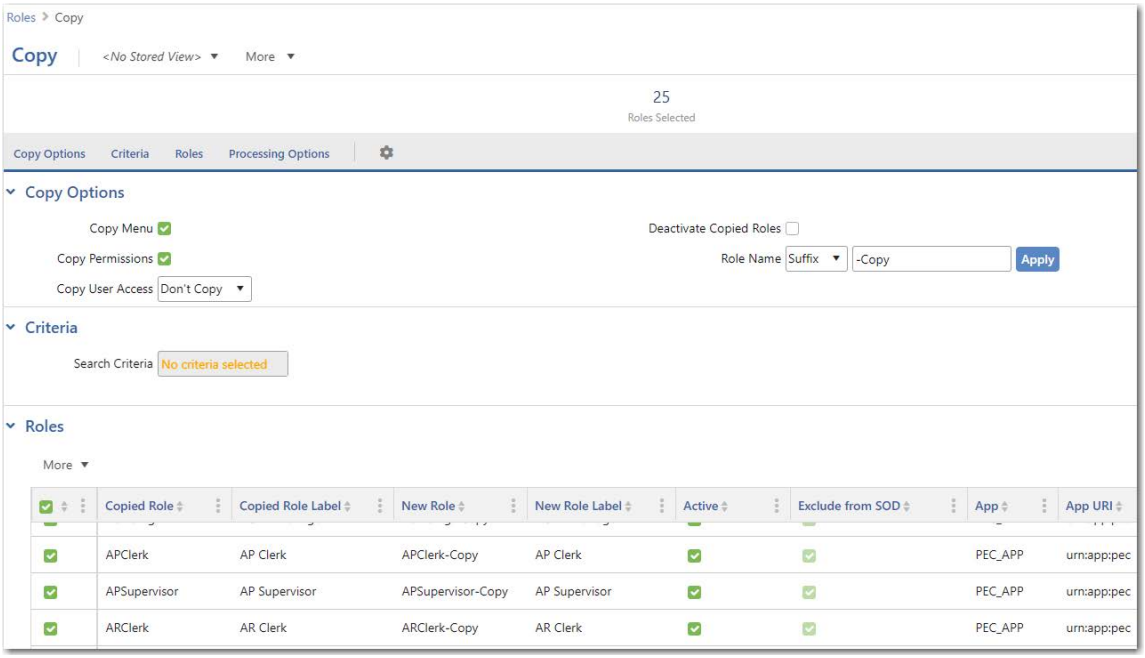
8 Assign permissions to the new role through role menus. See “Role Menus” on page 129.

Copy an Adaptive UX Role

The Copy action in Roles lets you copy a role's QAD Adaptive ERP and Adaptive UX permissions, and, optionally, copy the users assigned to the role and assign them to the new role. You have the option to not copy the user assignments, to replicate the user assignments from the copied role to the new role, or to move the user assignments from the copied role to the new role.

In the Roles browse, use the search criteria to identify the roles that you want to copy and, in the Actions menu, select Copy. The Copy window opens.

Fig. 6.6
Copy Window



The Copy window contains four panels: Copy Options, Criteria, Roles, and Processing Options (not shown in the screenshot).

Copy Options Panel

Copy Menu. This field is selected by default and copies the roles' associated menus.

Copy Permissions. This field is selected by default and copies the roles' Adaptive ERP and Adaptive UX permissions.

Copy User Access. Select an option to indicate how you want to treat users assigned to the copied roles. The options are:

- Don't Copy: Select this option if you do not want to assign users from the copied role to the new role.
- Copy: Select this option to copy the users assigned to the copied role to the new role. This value is the default.

- Copy & Replace: Select this option to replace user assignment to the copied role with the new role. This option supports scenarios such as where you want to copy and replace QAD roles with your own company's roles.

Note For some roles, such as the following, you cannot replace the user access: SuperUser, QADAdmin, WebUI_User, admin role set in Security Control, and Adaptive ERP roles (that have no App URI).

Deactivate Copied Roles. Select this field to deactivate the copied roles. This field is cleared by default.

Note You cannot deactivate some roles such as the following: SuperUser, QADAdmin, WebUI_User, admin role set in Security Control, and Adaptive ERP roles (that have no App URI).

If you attempt to deactivate a role, the system displays a warning message.

Role Name. Use this field to assign a prefix or a suffix to the copied role name to use as the new role name or to use a blank role name to allow manual entry of the new name.

Note In this field, you are setting the default value for the New Role field in the Roles panel grid. See "Roles Panel" on page 97.

Select an option from the following:

- Prefix: Select this option to add a prefix to the copied role name. If needed, the system removes letters from the end of the role name, after the prefix, to adhere to the 20-character role name limitation. If the system must truncate a role name for it to fit the character limitation, a message advises you of this. After you click Apply, for each selected row, the system copies the text in the Copied Role column to the New Role column, and adds the prefix.
- Suffix: Select this option to add a suffix to the copied role name. If needed, the system removes letters from the end of the copied role name, before the suffix, to adhere to the 20-character role name limitation. If the system must truncate a role name for it to fit the character limitation, a message advises you of this. After you click Apply, for each selected row, the system copies the text in the Copied Role column to the New Role column, and adds the suffix.

  This value is the default.
- Blank: After you click Apply, for each selected row, the system makes the New Role column blank. You can then manually enter a name for each role.

Criteria Panel

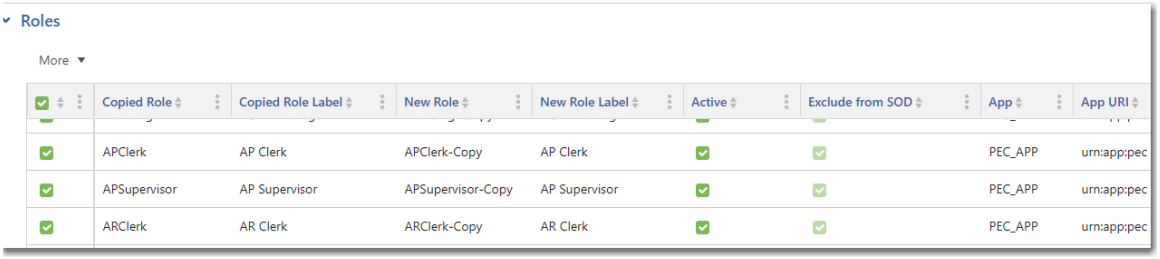
Search Criteria. This field displays the search criteria passed from the browse.

If no criteria are passed, the field displays "No Criteria Selected."

Roles Panel

The grid in the Roles panel displays roles from the browse, filtered by the search criteria. All roles are selected by default. Clear the checkboxes on the left for the roles that you do not want to copy.

Fig. 6.7
Roles Panel with Grid



Selected. The fields in the column are selected by default. Clear the field for a particular role if you do not want to copy the role.

Copied Role. This field displays the copied role name.

Copied Role Label. This field displays the copied role label.

New Role. This field displays the default value for this field, based on the option (Suffix, Prefix, or Blank) that you selected in the Role Name field in the Copy Options panel. The New role field has a character limit of 20.

New Role Label. This field displays the copied role label.

Active. This field is selected by default.

Exclude from SOD. This field is read only and is always selected and non-editable.

Important Copied roles are excluded from Segregation of Duties. You can manually change this setting in the Roles screen after the copy is complete.

App. This field is read only and set to “Configuration Data.”

App URI. This field is read only and set to “urn:app:pec.”

Namespace. This field is read only and set to “pec.”

Processing Options Panel

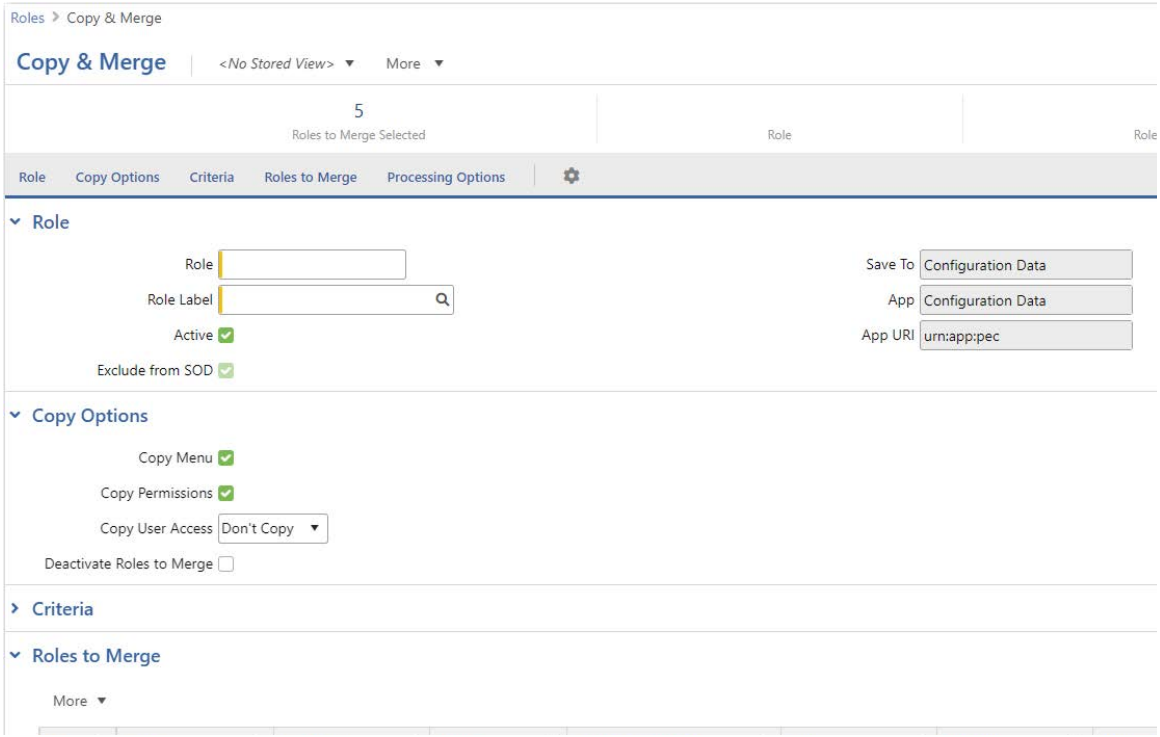
The Processing Options panel includes one field, Process in Background, which is always selected and read only. When you have configured your role copy options, click Submit to submit the copy action for processing. The system displays a message to indicate that the results will be sent to your inbox.

Copy and Merge Adaptive UX Roles

The Copy & Merge bulk action lets you copy the menus, permissions, and user access from multiple roles and to merge them in a new role. As with the Copy action, you have the option to copy the user assignments.

In the Roles browse, use the search criteria to identify the roles that you want to copy and merge and, in the Actions menu, select Copy & Merge. The Copy & Merge window opens.

Fig. 6.8
Copy & Merge Window



The Copy & Merge window contains five panels: Role, Copy Options, Criteria, Roles to Merge, and Processing Options (not shown in the screenshot).

Note The Criteria, Roles to Merge, and Processing Options panels are as described for the Copy action. See “Criteria Panel” on page 97, “Roles Panel” on page 97, and “Processing Options Panel” on page 98.

Role Panel

Role. Specify up to 20 alphanumeric characters for the new role to which the other roles will be copied and merged. The default is blank.

Role Label. Use the lookup to select the label string code. The default is blank.

Active. This field is selected by default. Clear the field to make the new role inactive.

Exclude from SOD. This field is read only and is always selected and non-editable.

Important Copied roles are excluded from Segregation of Duties. You can manually change this setting in the Roles screen after the copy and merge is complete.

Save To, App. These fields are read only and set to “Configuration Data.”

App URI. This field is read only and set to “urn:app:pec.”

Copy Options Panel

Copy Menu. This field is selected by default, and copies and merges the menus associated with the existing roles identified in the Roles to Merge grid. Any duplicates are removed during the merge. Clear the field if you do not want to copy the menus associated with the roles.

Copy Permissions. This field is selected by default, and copies and merges the Adaptive ERP and Adaptive UX permissions associated with the roles identified in the Roles to Merge grid. Clear the field if you do not want to copy the permissions associated with the roles.

Copy User Access. Select an option to indicate how you want to treat users assigned to the copied and merged roles. The options are:

- Don't Copy: Select this option if you do not want to assign users from the copied and merged roles to the new role. This option is the default.
- Copy: Select this option to assign the superset of all users assigned to the copied and merged roles to the new role. When the copy and merge action is complete, the users are assigned to the copied and merged roles, and the new role.
- Copy & Replace: Select this option to assign the superset of all users assigned to the copied and merged roles to the new role. The users' access to the roles that were copied and merged is removed.

Note For some roles, such as the following, you cannot replace the user access: SuperUser, QADAdmin, WebUI_User, admin role set in Security Control, and Adaptive ERP roles (that have no App URI).

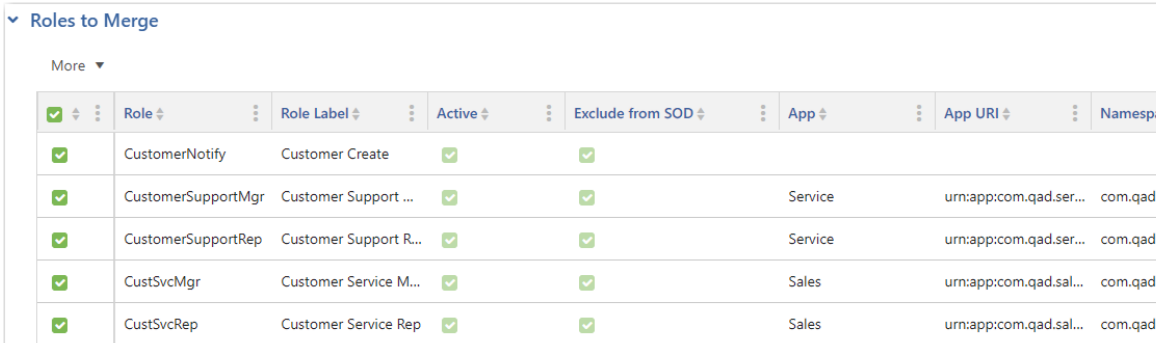
Deactivate Roles to Merge. Select this field to deactivate the roles to merge. This field is cleared by default.

Note You cannot deactivate some roles such as the following: SuperUser, QADAdmin, WebUI_User, admin role set in Security Control, and Adaptive ERP roles (that have no App URI).

Roles to Merge Panel

The grid in the Roles to Merge panel displays roles from the browse, filtered by the search criteria. All roles are selected by default. Clear the checkboxes on the left for the roles that you do not want to copy and merge.

Fig. 6.9
Roles to Merge Panel, with Grid



The grid fields are as described in the Roles panel for the Copy action. See “Roles Panel” on page 97.

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.

Note For Adaptive UX roles, use Role Menus to assign permissions. See “Role Menus” on page 129.

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, Master Comment Maintenance (`gpcmmts.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 gpcmmts.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.

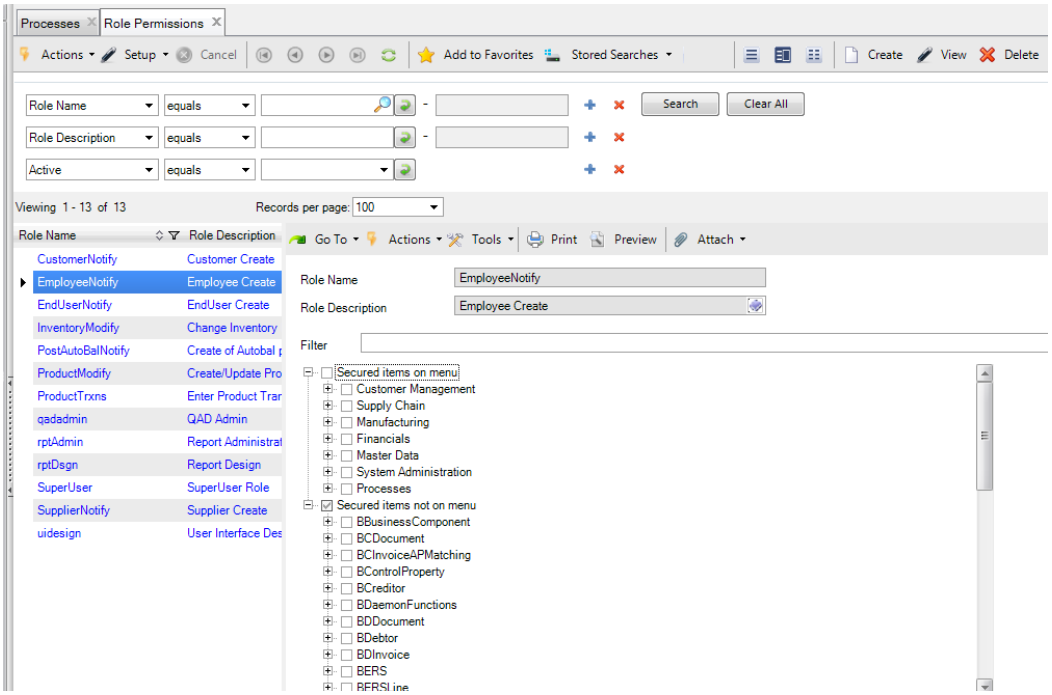
Role-based permission prevents any executable from being run from within your QAD application unless it is added to the menu and then added to a role. You cannot directly invoke a Progress program that is not on the menu by typing its name at the menu prompt in the character user interface.

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 Adaptive ERP, 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 6.10 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. 6.10
Role Permissions Maintain (36.3.6.5)

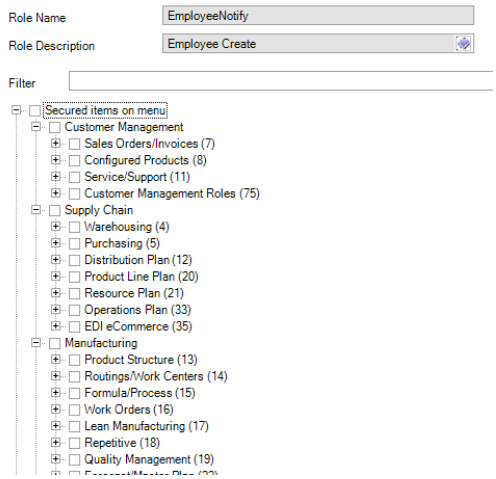


Secured Items on Menu

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 checkbox next to the item.

Fig. 6.11
Role Permissions Maintain, Secured Items on Menu



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 checkbox next to the item.

Fig. 6.12
Role Permissions Maintain, Secured Items Not on Menu

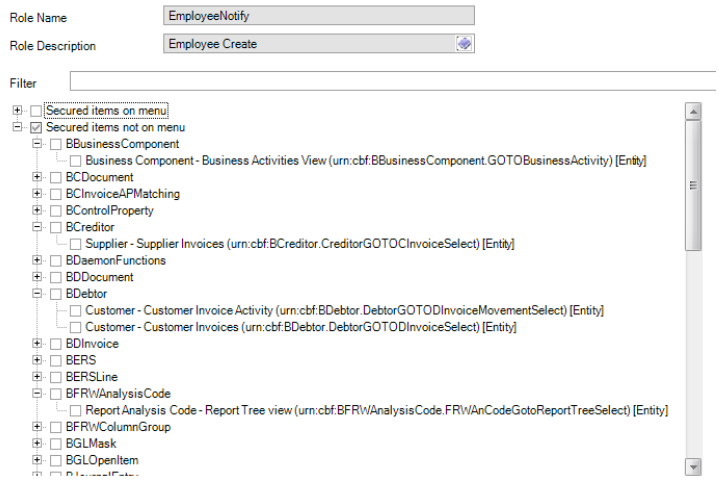


Table 6.1 on page 90 lists these functions and explains their use.

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*.

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 in the QAD Adaptive ERP or Users in Adaptive UX, 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 Adaptive ERP 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 Adaptive ERP and a corporate LDAP directory. Users can be synchronized using both the QAD Adaptive ERP and Adaptive UX.

User and group synchronization allows you to simply 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 5, “Authentication,” on page 57 for details on setting up LDAP and “Verify LDAP Instance Definition for DSML Gateway Using User Sync” on page 65 for details on user synchronization.

Once users are synchronized, continue setting up users with “Specify Access to Domains and Entities” on page 115.

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 Adaptive ERP administrative functions, that again needs access to all system resources.

- If you are using other components of QAD Adaptive 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) in the QAD Adaptive ERP or Users in Adaptive UX to assign a unique ID to a system user and define related application and security details.

Note Adaptive UX often combines multiple Adaptive ERP programs into one screen. Both interfaces require the same data to create a new user profile, but the order in which that information is requested varies by interface. Screenshots from both interfaces are displayed in this section to give additional context.

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 checkbox and the Enabled checkbox in User Maintenance have different functions.

- The Active checkbox 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 checkbox determines whether a user can sign in. By default, the Enabled checkbox is selected when a new user is created. A user can sign in to the system only if both the Enabled checkbox and Active checkbox 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. 6.13
Adaptive ERP User Maintenance (36.3.1)

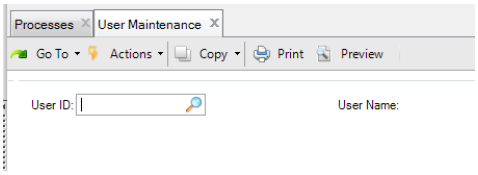
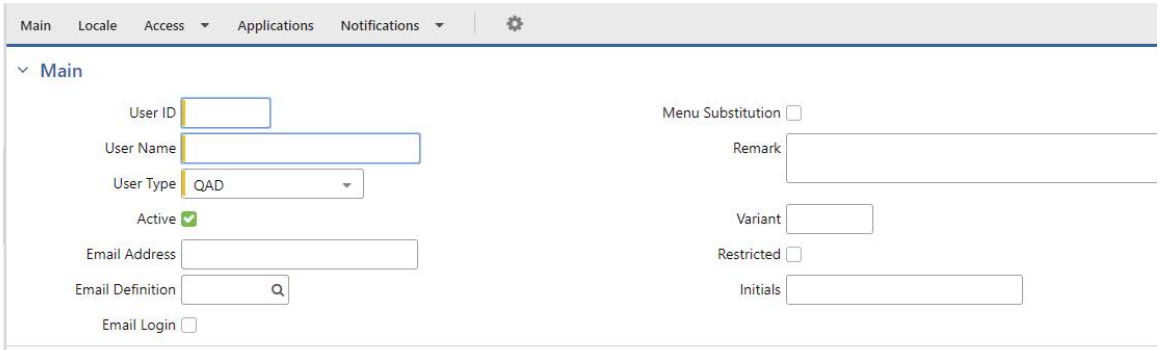


Fig. 6.14
Adaptive UX Users (Main Panel)



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 (!), commas (,) or forward and backward slashes (/ \). 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 Adaptive ERP 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 Adaptive ERP, the user ID always displays in the bottom message area. See “Header Display Mode” on page 29.

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 email 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. 6.15
Adaptive ERP User Maintenance, Language and Country Code

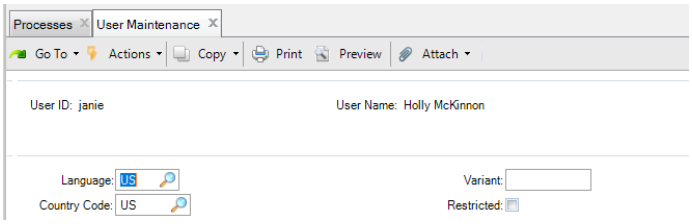


Fig. 6.16
Adaptive UX Users (Locale Panel)

Language. Enter or select 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. The Variant setting is located with the Main panel in Adaptive UX.

Information on language, country code, and variant are maintained in a file named `locale.dat`, along with other format information. Once the system determines a user's language, country code, and corresponding ISO country code, it gets information from `locale.dat` and uses it to set user-specific date and number formats.

System administrators may need to change information in `locale.dat` or add entries for countries that are not included in the current file.

Each line in the file follows the same format. For example, the line for US English looks like this:

```
US,en,US,,mdy,American
```

Where:

- US is the 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. 6.17
Adaptive ERP User Maintenance, User Identity Fields

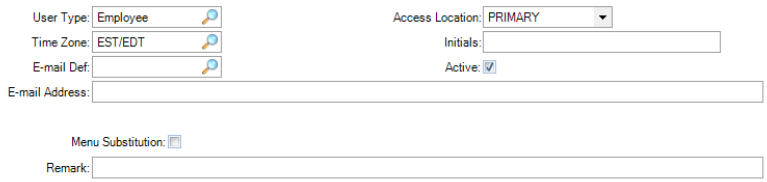
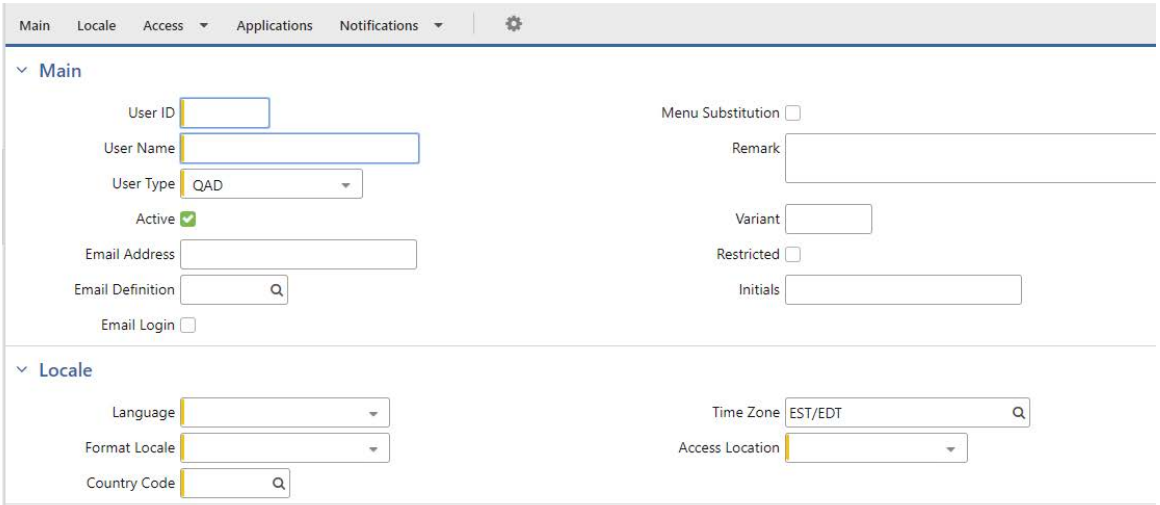


Fig. 6.18
Adaptive UX Users (Main and Locale Panels)



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 checkbox 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 Email Addresses

Associate a valid email 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 email address.

Email 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 email.

  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 electronic signatures, use e-mail to inform administrators of unusual system events.

Enable Menu Substitutions

Select the Menu Substitution checkbox 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 Adaptive ERP or Adaptive UX.

Enable Active Directory Access

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

Note As of the Enterprise Edition 2018 release, only server-side Active Directory authentication is supported. Client-side Active Directory authentication is no longer supported.

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. This username is limited to 64 characters.

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. 6.19
Adaptive ERP User Maintenance, System Access Frame

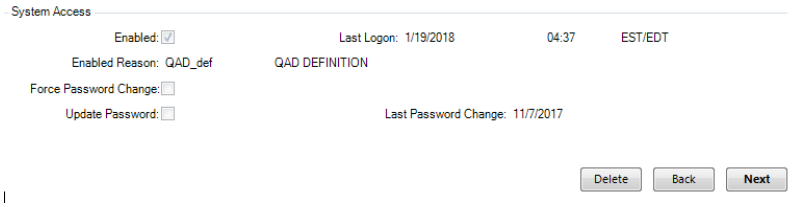


Fig. 6.20
Adaptive UX Users (Access Panel)

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

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

Note Any time this checkbox 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 checkbox; 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 30.
- 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 31.

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 checkbox for new users and the checkbox cannot be updated. This lets you assign temporary, single-use passwords either automatically or manually.

By default, the system clears this checkbox 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 checkbox 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 checkbox by default, and you cannot change it.

Update Passwords

When the Update Password checkbox 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 emails 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. 6.21
QAD Adaptive ERP User Maintenance, Set New Password Frame

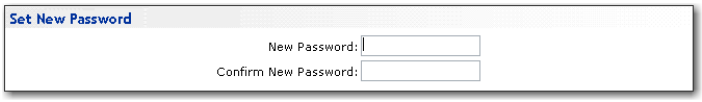
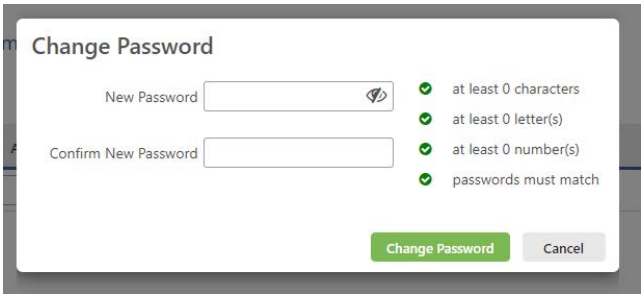


Fig. 6.22
Adaptive UX Users (Change Password Frame)



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 33.

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 29.

- 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 checkbox, the Active checkbox is selected for all licensed applications for this user. Otherwise, QAD Adaptive Applications (MFG/PRO) is listed as the only active application. You can list additional licensed software applications, then select (or clear) the Active checkbox for each application. By default the checkbox is selected.

Fig. 6.23
Adaptive ERP User Maintenance, Application List Frame

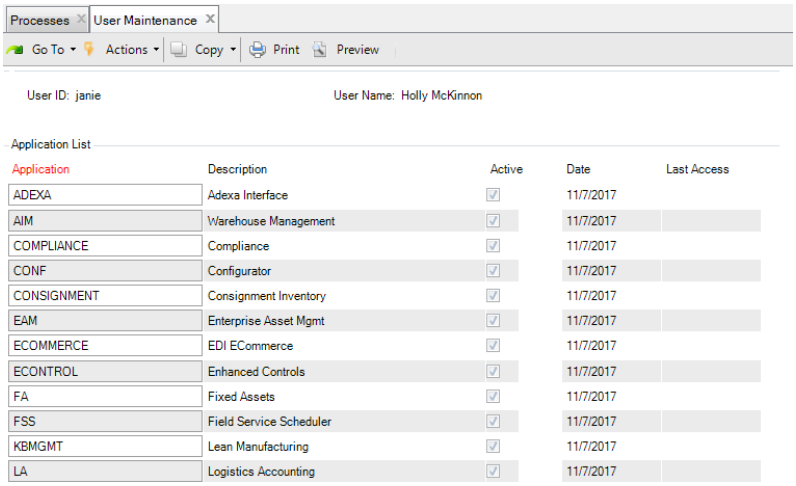
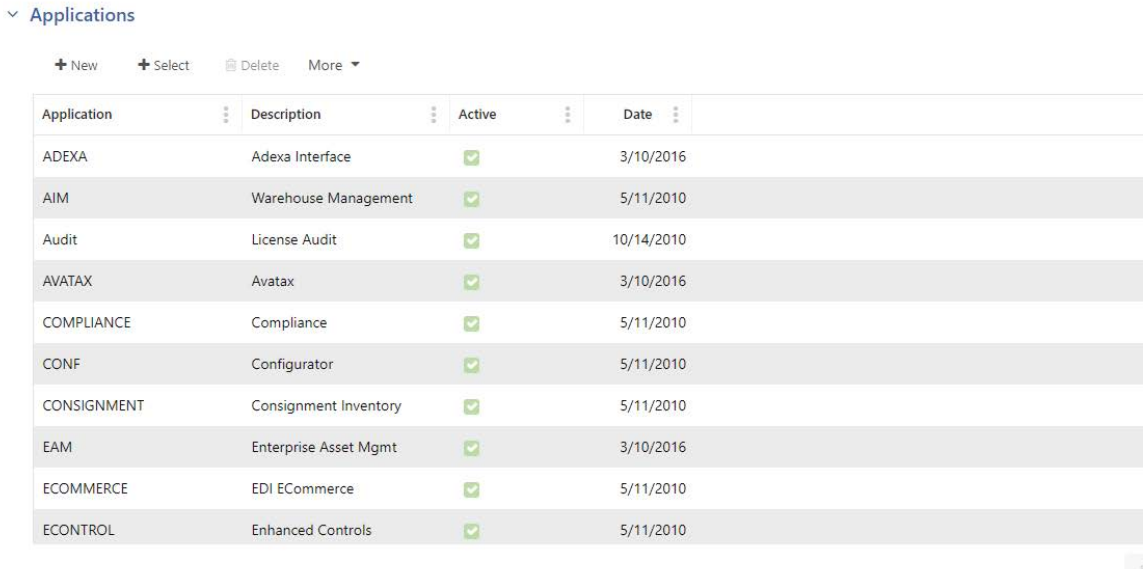


Fig. 6.24
Adaptive UX, Applications Panel



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.

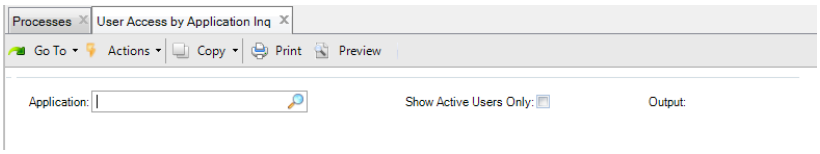
The system counts the number of enabled users authorized to access the application and compares the number against a predefined limit for your license type. If the number of enabled users exceeds the predefined limit, a violation message displays and you cannot add the application to the list.

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

If you disable the Adaptive 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. 6.25
User Access by Application Inquiry (36.3.23.4)



Specify Access to Domains and Entities

To create or maintain user access privileges for domains and entities, use User Domain/Entity Access Maintain (36.3.4) in the QAD Adaptive ERP or User Access in Adaptive UX. The combination of domain and entity represents a workspace.

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 in the Adaptive ERP and User Access in Adaptive UX. You must explicitly grant users access before any updates can be made in the new domain.

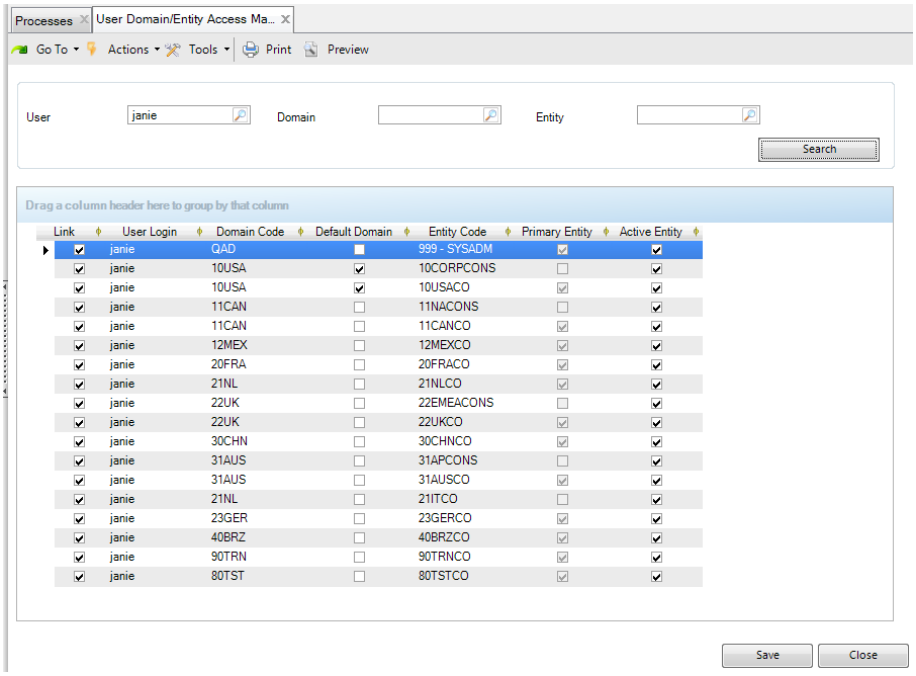
Any changes to a user's domain or entity access privileges automatically update that user's role membership information. For example, removing a user's ability to access an entity breaks the association between that entity and the user's assigned role, and the entity is deleted from the list of assigned entities in Role Membership Maintain (36.3.6.6.1). For details on role membership see "Define Role Membership" on page 119.

Assign Access in the QAD Adaptive ERP

User Domain/Entity Access Maintain provides a workbench type screen in the QAD Adaptive ERP 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 checkbox in the Select column indicates that the user has access to the associated combination of domain and entity.

Fig. 6.26
User Domain/Entity Access Maintain



You can also modify the user's default domain by selecting the Default Domain checkbox. 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 checkbox on the row of the user's default domain. Only one domain can be designated as default. In the QAD Adaptive ERP, 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.

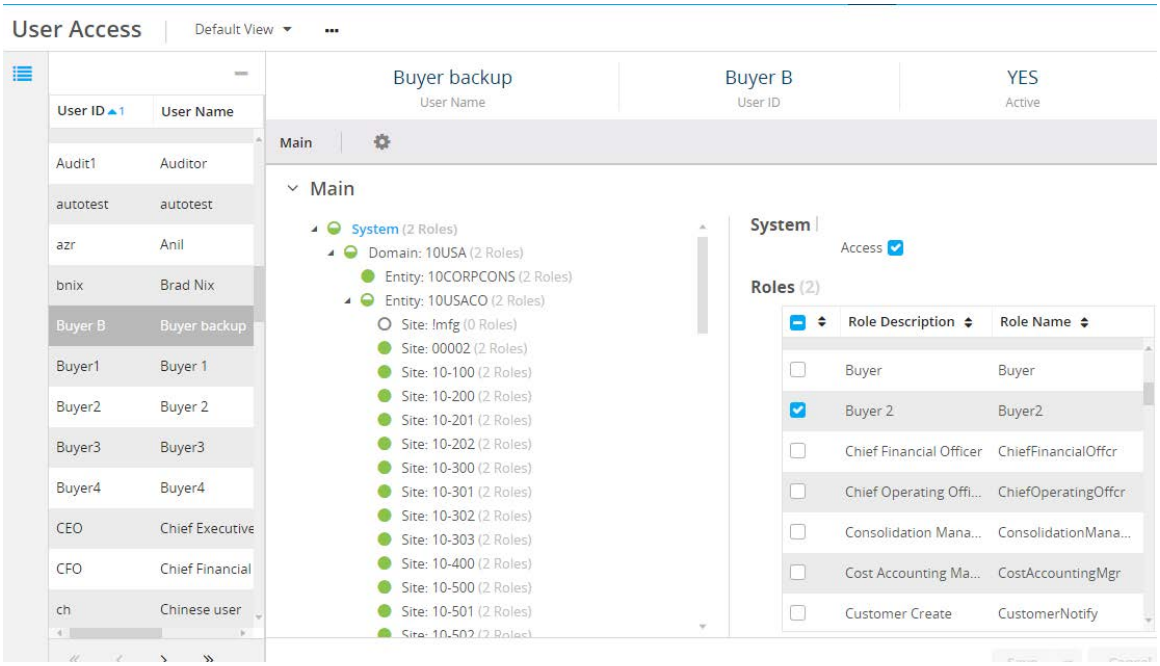
Users employing the QAD Adaptive ERP can switch entities by opening a different workspace.

Assign Access in Adaptive UX

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. Every Adaptive UX user must be assigned at least two roles, one of which is webui_user. A user cannot access Adaptive UX without the webui_user role, but can still access the QAD Adaptive ERP.

Note Users who access the QAD Mobile Action Center App also must be assigned the webui_user role. If QAD Mobile App users are not assigned to the webui_user role, they may run into permission errors for requisitions and generic approval configuration resources.

Fig. 6.27
User Access



Set System Access

Set access to domains, entities, and sites by selecting or clearing the Access checkbox, located above the Roles grid, for the appropriate system level.

Note Modifying site security on the User Access screen does not change site security settings in the QAD Adaptive ERP or on Site Security in the QAD Adaptive UX.

The System tree is a hierarchical view of all domains, entities, and sites within Adaptive UX. Each level of the tree shows the number of roles the selected user belongs to at that level and a circular status indicator denotes the user's access to that level and its children. A solid green circle denotes access to that node and all nodes lower in the tree. A white circle with a gray border indicates that the user has no access to the associated node, nor to that node's children. A half-green circle indicates that the user has access to some but not all of the nodes lower in the tree. Sites are the lowest level of the hierarchy and can only have full access or no access.

Inheritance of access runs both up and down the tree. Enabling access to a node automatically enables access to the node's parent and children. Removing access to a child does not affect the parent. You can remove the access for nodes lower in the tree by clearing the Access checkbox for those child items one by one. If you clear the Access checkbox of a parent element, you cannot select the Access checkbox of a child element.

In Figure 6.27, 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 children.

Define Role Membership

Use Role Membership Maintain (36.3.6.6) in the QAD Adaptive ERP and User Access in the QAD Adaptive UX 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 89 for details.

Note Users must be assigned to roles using both Role Membership Maintain in the QAD Adaptive ERP and User Access in Adaptive UX in order to access both interfaces. Assigning a user to a role in the QAD Adaptive ERP does not grant that user access to QAD Adaptive UX.

QAD Adaptive ERP Role Membership Maintain

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.

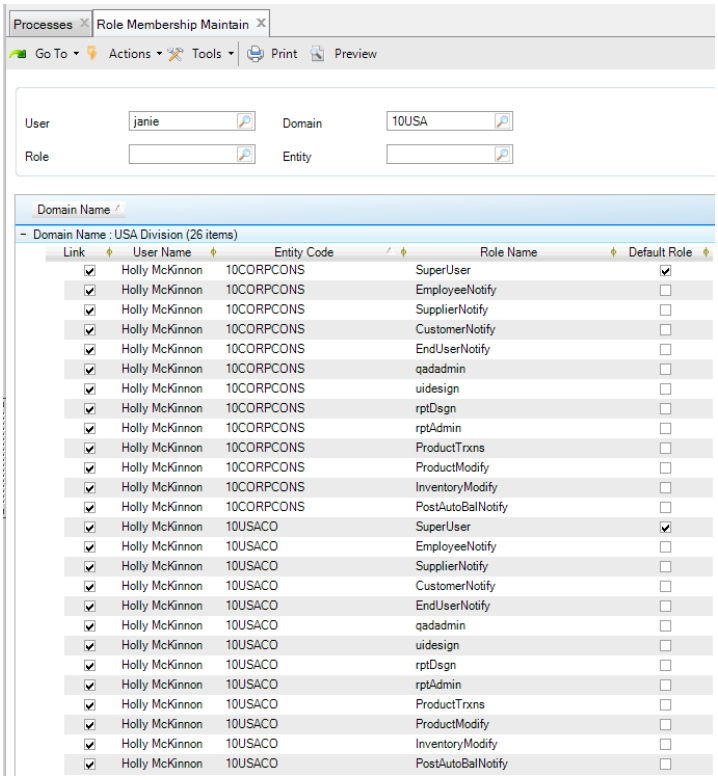
Specifying role membership defines both who belongs to the role and the *role context*; that is, which domains and entities the role can access.

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. 6.28
Role Membership Maintain (36.3.6.6)



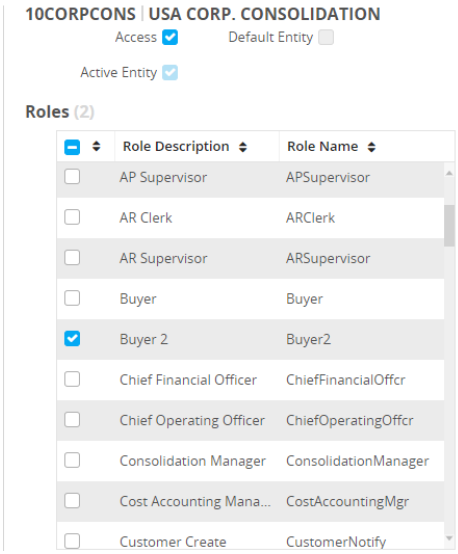
Use the User, Role, Domain, and Entity fields at the top of the screen to select the records you want to work with during this session. You can group the data in the grid or sort or rearrange columns to streamline the setup activity. Selecting the checkbox indicates that the user has access to the role 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 115.

QAD Adaptive UX User Access Roles Grid

The Roles grid on User Access displays all of the roles in QAD Adaptive UX. You can only edit the Roles grid when the Access checkbox is selected for the associated domain, entity, or site. Select the checkbox next to a role to assign the user to that role. Clear the checkbox next to a role to remove the user from that role.

Fig. 6.29
Roles Grid



Inheritance of role membership runs both up and down the tree. Selecting a role at any level automatically adds the role to the node's parent and children. Removing a role automatically removes the role from the node's children. However, you can remove a role from a child node and leave the role selected at the parent node.

Figure 6.29 shows the roles in entity 10CORPCONS. You can modify role assignments for the selected user using the Roles grid.

View Access Information

The following view programs display security-related information in the QAD Adaptive ERP. In QAD Adaptive UX, view security-related information on User Access, Roles, and Role Permissions.

- 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

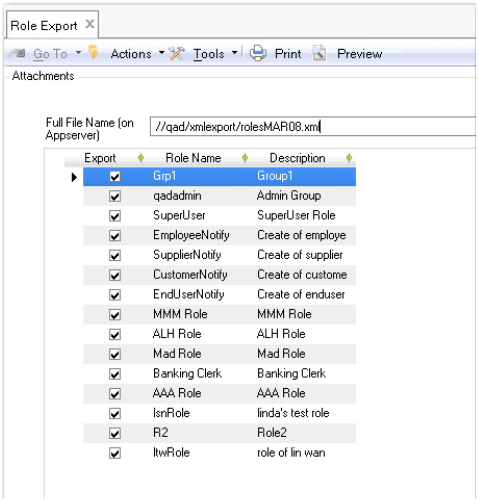
The default roles available in the system are loaded from the file `defaultroles.xml` during the initial install or as part of a system synchronization or update.

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. 6.30
Role Export



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

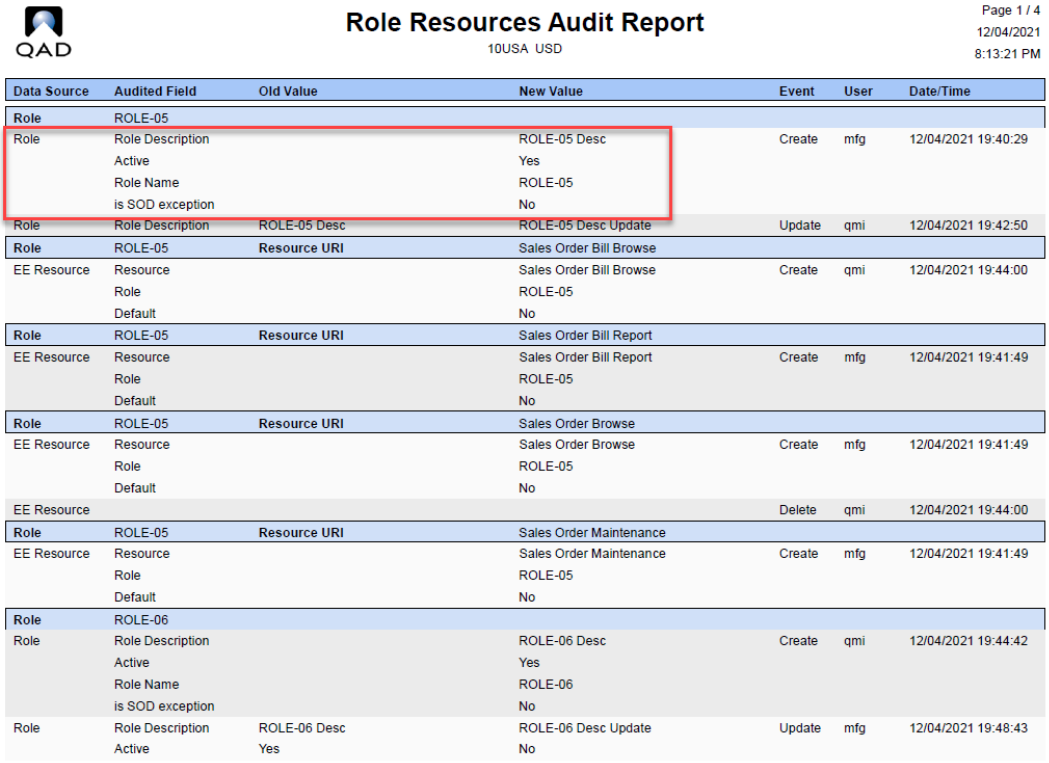
Select the roles to be exported and click Export.

Role and User Audit Reports

You can generate two audit trail reports to review changes made to roles, role permissions, users, user licenses, and user access.

The Role Resource Audit Report tracks changes made to a role record as well as to a role's role permissions, both in Adaptive UX and Adaptive ERP.

Fig. 6.31
Role Resource Audit Report



QAD

Role Resources Audit Report

10USA USD

Page 1 / 4
12/04/2021
8:13:21 PM

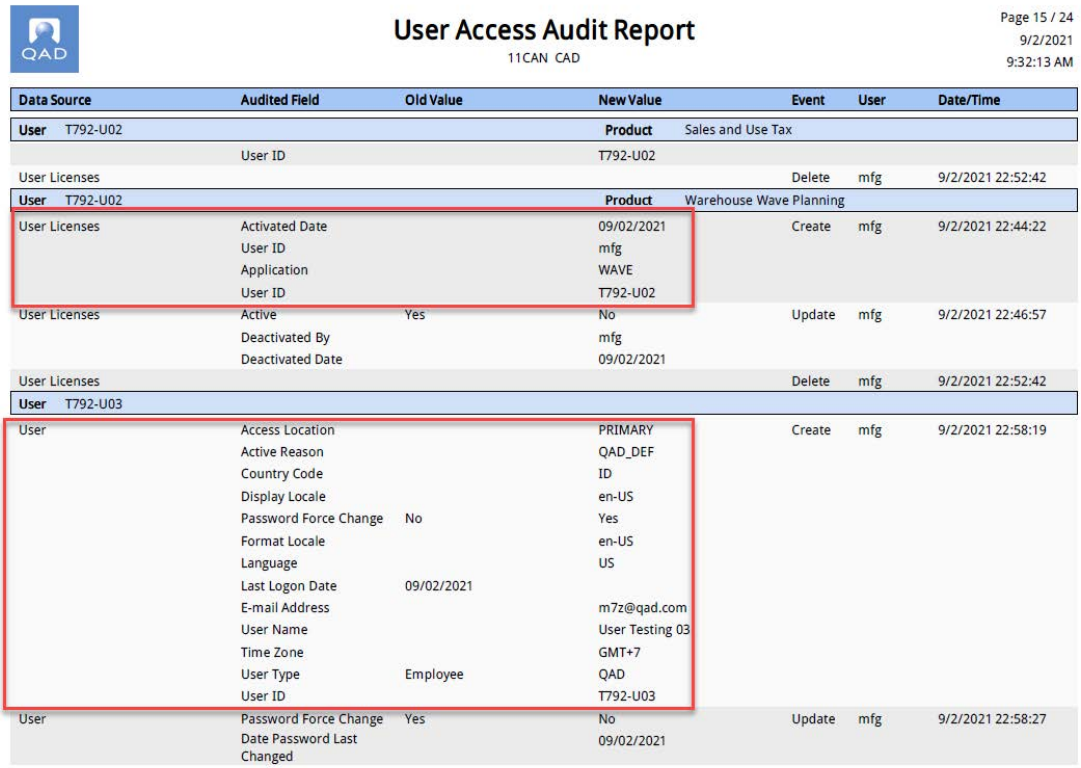
Data Source	Audited Field	Old Value	New Value	Event	User	Date/Time
Role	ROLE-05					
Role	Role Description		ROLE-05 Desc	Create	mfg	12/04/2021 19:40:29
	Active		Yes			
	Role Name		ROLE-05			
	is SOD exception		No			
Role	Role Description	ROLE-05 Desc	ROLE-05 Desc Update	Update	qmi	12/04/2021 19:42:50
Role	ROLE-05	Resource URI	Sales Order Bill Browse			
EE Resource	Resource		Sales Order Bill Browse	Create	qmi	12/04/2021 19:44:00
	Role		ROLE-05			
	Default		No			
Role	ROLE-05	Resource URI	Sales Order Bill Report			
EE Resource	Resource		Sales Order Bill Report	Create	mfg	12/04/2021 19:41:49
	Role		ROLE-05			
	Default		No			
Role	ROLE-05	Resource URI	Sales Order Browse			
EE Resource	Resource		Sales Order Browse	Create	mfg	12/04/2021 19:41:49
	Role		ROLE-05			
	Default		No			
EE Resource				Delete	qmi	12/04/2021 19:44:00
Role	ROLE-05	Resource URI	Sales Order Maintenance			
EE Resource	Resource		Sales Order Maintenance	Create	mfg	12/04/2021 19:41:49
	Role		ROLE-05			
	Default		No			
Role	ROLE-06					
Role	Role Description		ROLE-06 Desc	Create	qmi	12/04/2021 19:44:42
	Active		Yes			
	Role Name		ROLE-06			
	is SOD exception		No			
Role	Role Description	ROLE-06 Desc	ROLE-06 Desc Update	Update	mfg	12/04/2021 19:48:43
	Active	Yes	No			

For role records, the report lists changes made to any of the fields on a role. If the role is new, the Old Value column is blank and the New Value column displays the initial record content. In Figure 6.31, you can see that ROLE 05 was created with the description of ROLE-05 Desc. It is an active role and is not exempt from segregation of duties.

The User Access Audit Report tracks changes made to:

- Users
- User Licenses
- User Access

Fig. 6.32
User Access Audit Report - Example 1



User Access Audit Report
11CAN CAD

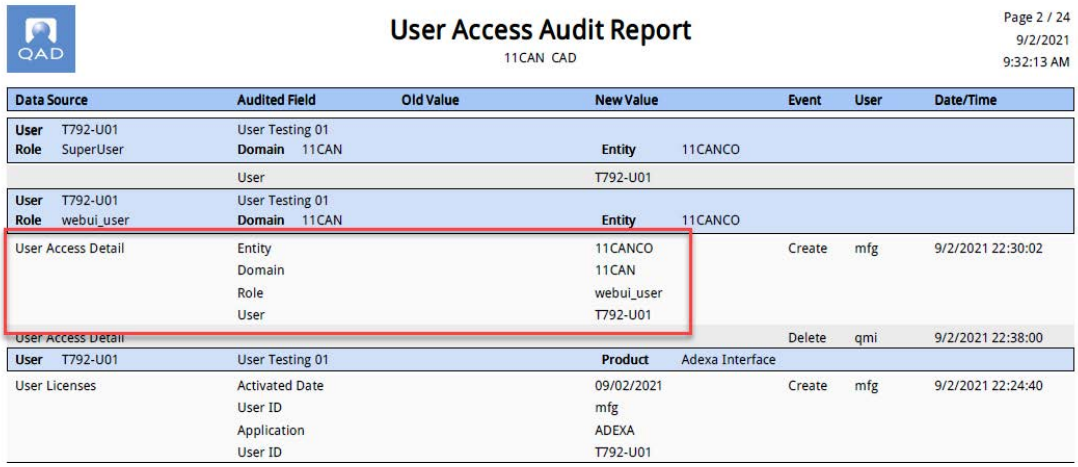
Page 15 / 24
9/2/2021
9:32:13 AM

Data Source	Audited Field	Old Value	New Value	Event	User	Date/Time
User T792-U02			**Product** Sales and Use Tax			
	User ID		T792-U02			
User Licenses				Delete	mfg	9/2/2021 22:52:42
User T792-U02			**Product** Warehouse Wave Planning			
User Licenses	Activated Date		09/02/2021	Create	mfg	9/2/2021 22:44:22
	User ID		mfg			
	Application		WAVE			
	User ID		T792-U02			
User Licenses	Active	Yes	No	Update	mfg	9/2/2021 22:46:57
	Deactivated By		mfg			
	Deactivated Date		09/02/2021			
User Licenses				Delete	mfg	9/2/2021 22:52:42
User T792-U03						
User	Access Location		PRIMARY	Create	mfg	9/2/2021 22:58:19
	Active Reason		QAD_DEF			
	Country Code		ID			
	Display Locale		en-US			
	Password Force Change	No	Yes			
	Format Locale		en-US			
	Language		US			
	Last Logon Date	09/02/2021				
	E-mail Address		m7z@qad.com			
	User Name		User Testing 03			
	Time Zone		GMT+7			
	User Type	Employee	QAD			
	User ID		T792-U03			
User	Password Force Change	Yes	No	Update	mfg	9/2/2021 22:58:27
	Date Password Last Changed		09/02/2021			

The report displays what permissions have been granted to or revoked from the specified resource. If the permissions were newly defined instead of changed, the Old Value column is blank and the New Value column displays the initial record settings.

The report in Figure 6.32 shows changes to both user licenses and a user record. The event detail highlighted in red for the user license shows the activation date for the listed application, WAVE, along with the user IDs of the user who activated the license and the user who now can use the application. The event detail highlighted for the user shows the fields that are tracked when a user record is created.

Fig. 6.33
User Access Audit Report - Example 2



User Access Audit Report
11CAN CAD

Page 2 / 24
9/2/2021
9:32:13 AM

Data Source	Audited Field	Old Value	New Value	Event	User	Date/Time
User T792-U01 **Role** SuperUser	User Testing 01 **Domain** 11CAN		**Entity** 11CANCO			
	User		T792-U01			
User T792-U01 **Role** webui_user	User Testing 01 **Domain** 11CAN		**Entity** 11CANCO			
User Access Detail	Entity		11CANCO	Create	mfg	9/2/2021 22:30:02
	Domain		11CAN			
	Role		webui_user			
	User		T792-U01			
User Access Detail				Delete	qmi	9/2/2021 22:38:00
User T792-U01	User Testing 01		**Product** Adexa Interface			
User Licenses	Activated Date		09/02/2021	Create	mfg	9/2/2021 22:24:40
	User ID		mfg			
	Application		ADEXA			
	User ID		T792-U01			

The User Access Audit Report also tracks changes to domains, entities, and sites on the User Access screen, as shown in Figure 6.33.

For more detailed information on audit trail reports and enabling auditing in your environment, see Chapter 13, “Auditing,” on page 329.

Chapter 7

Adaptive UX Security

This chapter applies only if you are using QAD Adaptive ERP with Adaptive UX. It covers the following topics:

Overview ***128***
Explains users, roles, and menus within Adaptive UX.

Prerequisites ***128***
Describes the prerequisites for using Adaptive UX.

Role and User Workflow in Adaptive UX ***128***
Describes the ideal workflow for introducing users and roles into Adaptive UX.

Resources ***128***
Explains Adaptive UX resources and how to secure resources.

Menus ***129***
Describes role and favorites menus and using menus to assign permissions to roles.

Role Permissions ***136***
Describes the Role Permissions screen and how to assign permissions to roles.

Role Resource Audit Report ***155***
Describes how to review changes made to role permissions for resources in Adaptive UX and Adaptive ERP.

Configure Stored Views Access ***157***
Explains how to save customized screen layouts, emphasizing important information needed for everyday use and specific tasks.

Record-Level Security ***158***
Explains how to enable record-level security and how to share secure records.

Overview

Creating and maintaining a secure environment for Adaptive UX requires initial steps that can be performed in both the QAD Adaptive ERP and Adaptive UX. Once these steps are complete, security can be maintained within the QAD Adaptive UX.

Prerequisites

You must be running QAD Adaptive ERP.

Important To manage roles, menus, and permissions in Adaptive UX 2023 environments, you must use new Configuration Data export.

Role and User Workflow in Adaptive UX

1. Create roles. See “Set Up Roles” on page 88.
2. Create role menus for the newly created roles and assign permissions to those role menus. See “Role Menus” on page 129.
3. Create system users. See “Set Up Users” on page 104.
4. Specify user access to domains, entities, and sites in User Access. See “Assign Access in Adaptive UX” on page 118.
5. Assign users to roles in User Access. All Adaptive UX users must be assigned to at least two roles, one of which is webui_user, before they can access the system. See “QAD Adaptive UX User Access Roles Grid” on page 120.
6. Configure settings for stored views, which allow users to customize screen layout. See “Configure Stored Views Access” on page 157.

Resources

Adaptive UX is made up of resources, which are uniquely identifiable pieces of the product that need to be secured. Securing resources limits access to specific roles that have adequate permission to interact with different areas of the system. All resources can be secured.

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

Adaptive UX Resources

The following resources can be secured in Adaptive UX.

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 Component. The business logic and data necessary to represent real-world elements, such as sales orders, within Adaptive UX.

Browse. The QAD Adaptive ERP, 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 component 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 component.

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

Menus

The Menus browse is a collection of all menus that exist in Adaptive UX environments. The browse displays all QAD-provided role menus, all non-QAD role menus, and all user favorites menus. Users see the menus for the roles to which they are granted access in Adaptive UX.

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 items are grouped in folders in a tree structure on the Menu panel of the hybrid view. The folder name appears on the Menu Bar and the folder contents, or pages, make up the associated drop-down menu.

Role Menus

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 Adaptive UX menu bar and users see a role menu for each role to which they are assigned that has a defined role menu.

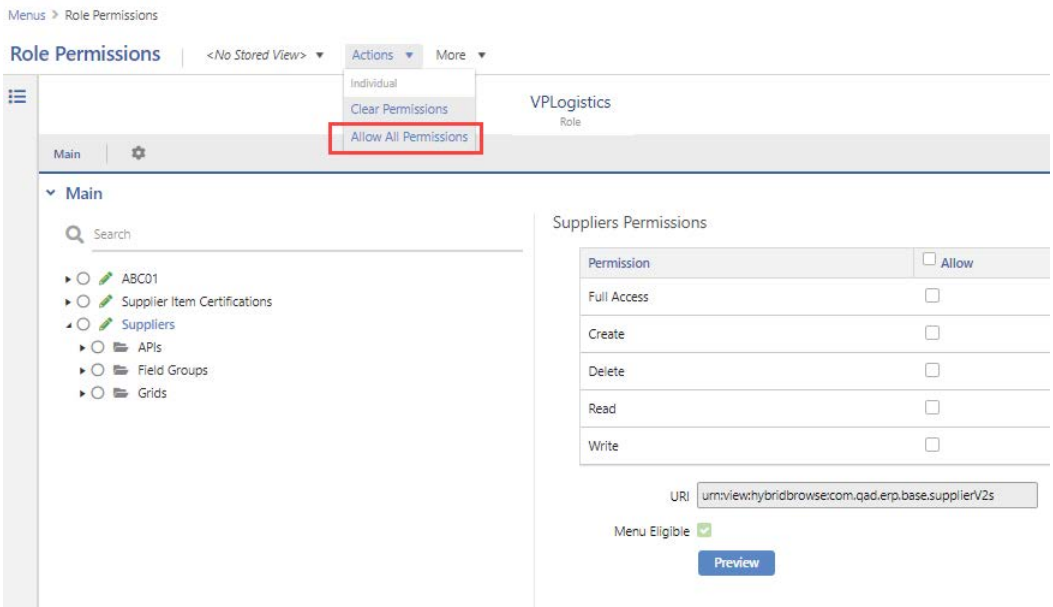
Create a New Role Menu

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, see “Create a New Adaptive UX Role” on page 95.

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.
   - Pages are the system’s menu items.
   - 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.

   Note All role menus appear on the mobile app for users who have mobile access. If a role does not require access to specific functions on the mobile app, clear the Include in Mobile App checkbox.
6. Save the populated role menu.
7. Select Permissions at the bottom of the screen. Role Permissions displays only the resources that make up the role menu you created. You must grant access to these resources for the role to have access to all required areas of Adaptive UX.

Fig. 7.1
Allow All Permissions



8. Select Allow All Permissions from the Actions menu and confirm the action by clicking OK.

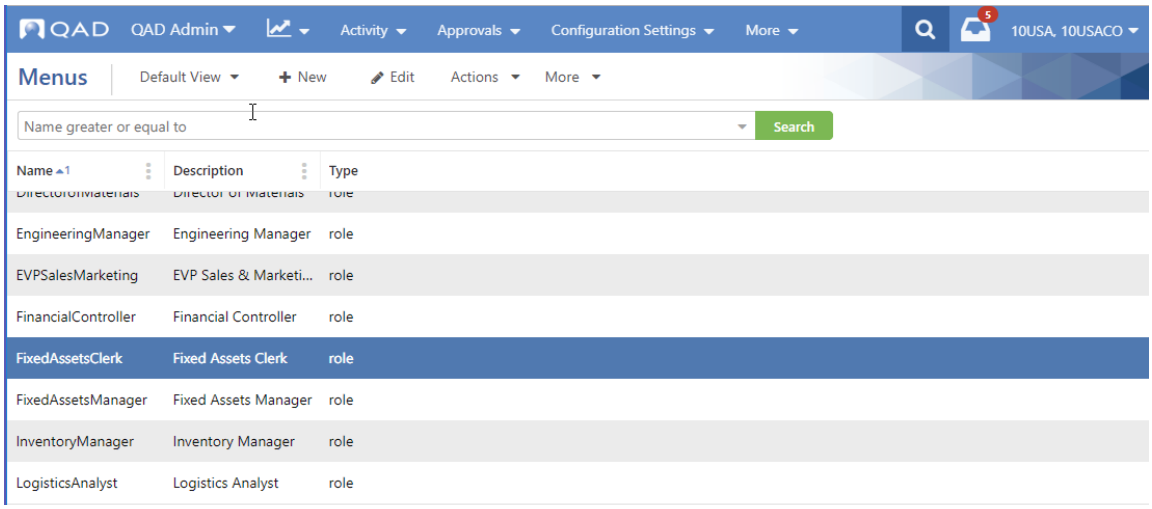
9 All of the secured resources should now have a green circle next to them. The system saves the setup automatically.

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, see “Create a New Adaptive UX Role” on page 95.

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

Fig. 7.2
Menus

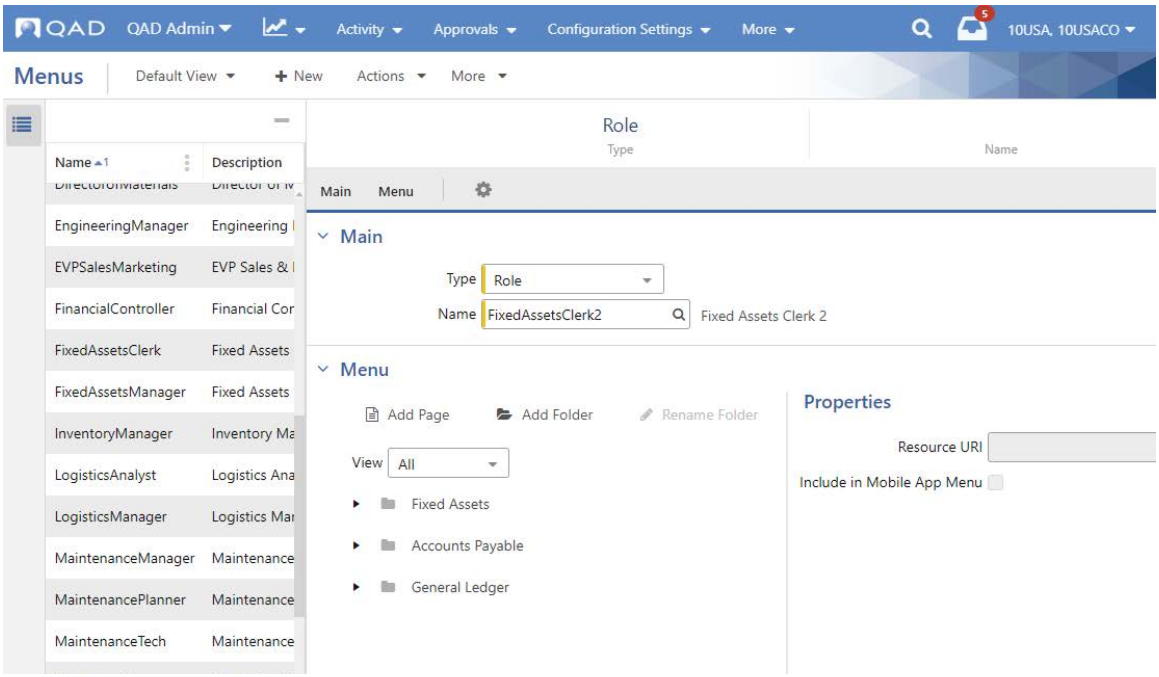


2 Select Copy from the Actions menu.

3 Select Role from the Type drop-down menu.

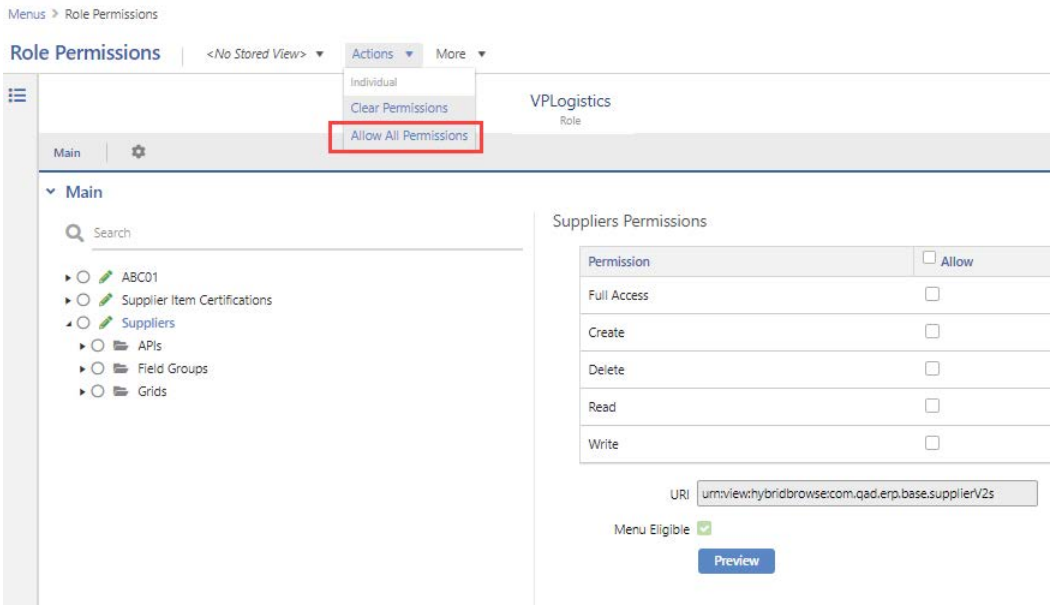
4 In the Name lookup, select the role that will be assigned this role menu.

Fig. 7.3
Copy a Role Menu



5 Select Save. Then select Permissions at the bottom of the screen. The Role Permissions window displays the resources that make up the role menu you copied. These resources need to be allowed access for the new role to have access to all required areas of Adaptive UX.

Fig. 7.4
Allow All Permissions



6 Select Allow All Permissions from the Actions menu and confirm the action by clicking OK.

7 All of the secured resources should now have a green circle next to them. The system saves the setup automatically.

Import EE Role Permissions

Use the Import EE Role Permissions action to create role menus and role permissions that align with EE role permissions. The action creates a set of menu-eligible resources in top-level folders based on the functional area. Those folders become the menu options in the menu bar of Adaptive UX. You can reorganize the menu items and set permissions directly from the Menus screen, or you can choose to have the system set permissions during import.

See “Import EE Role Permissions” on page 145 for more details on this action.

Favorites Menu

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

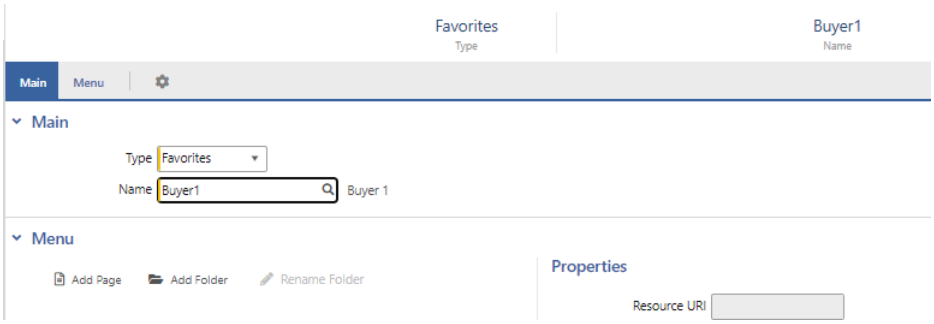
Create a New Favorites Menu for a User

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 menu.

Fig. 7.5
Create New Favorites Menu



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 Click Save.

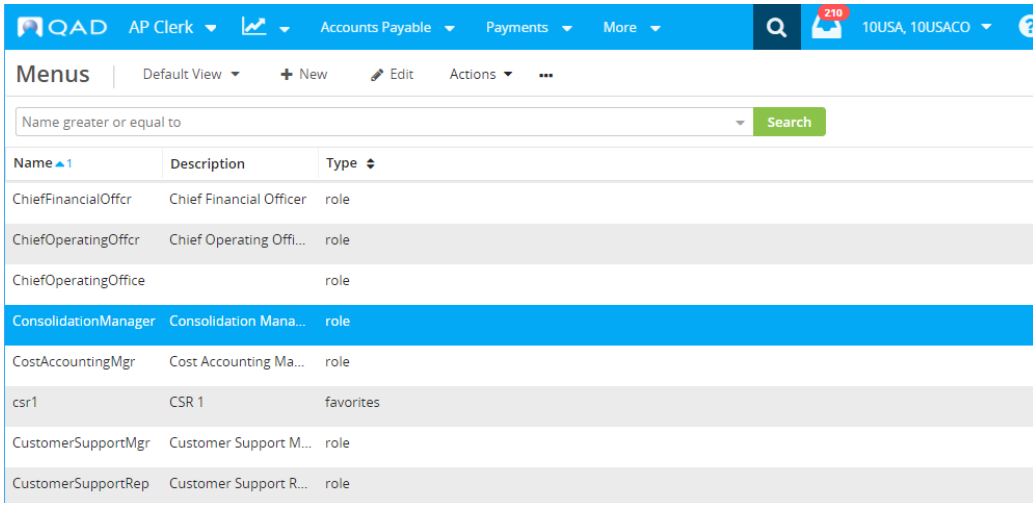
6 Click Permissions to check that the user's role has adequate permission to access the newly assigned Favorites menu. If all resources are not green, you can choose Allow All Permissions from the Actions menu. but remember that you are updating the resources for the role, not just this user.

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 menu you want to copy.

Fig. 7.6
Menus



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 Click 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.

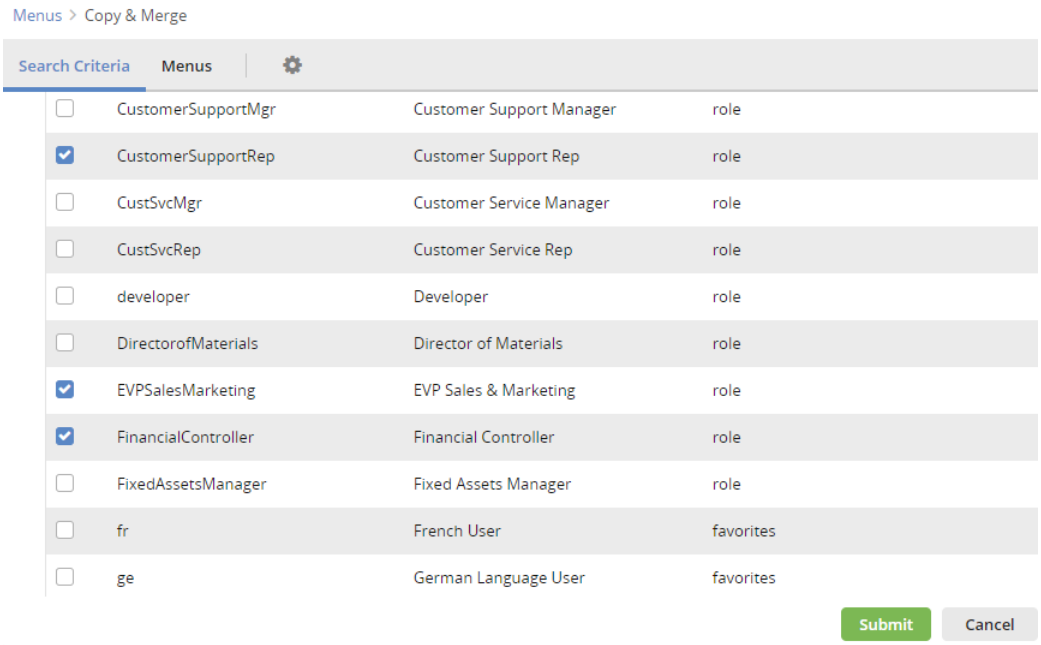
Copy and Merge Multiple Menus

Use the Copy and Merge action to create a new menu by combining multiple existing menus. This action is available from the Actions menu on the Menus browse, not the hybrid view. If you only see Copy in the Actions menu, close the hybrid view so you only see the list of menus.

1 Select Copy and Merge from the Action menu.

2 Clear all of the menu checkboxes by clearing the Name option at the top of the list. Select the role menus you want to merge.

Fig. 7.7
Copy and Merge



3 Click Submit.

4 Select the type of menu you are creating, either Role or Favorites

5 Select the name from the lookup of the role to which to assign this menu.

6 Assign the permissions by clicking the blue Permissions button.

Note You cannot have duplicate resources in the new menu, and the system does not resolve duplicates. If your combined menu has resources listed in multiple places, you will receive an error if you try to save the new menu. Find the duplicates in the Menu panel and delete them.

7 Save the new menu.

Role Permissions

You can access the Role permissions information in the following ways:

- From the main Role Permissions screen
- From the Menus screen: by clicking the Permissions button in the bottom right corner of a screen
- From other screens: by selecting the Permissions option from the More drop-down in the toolbar

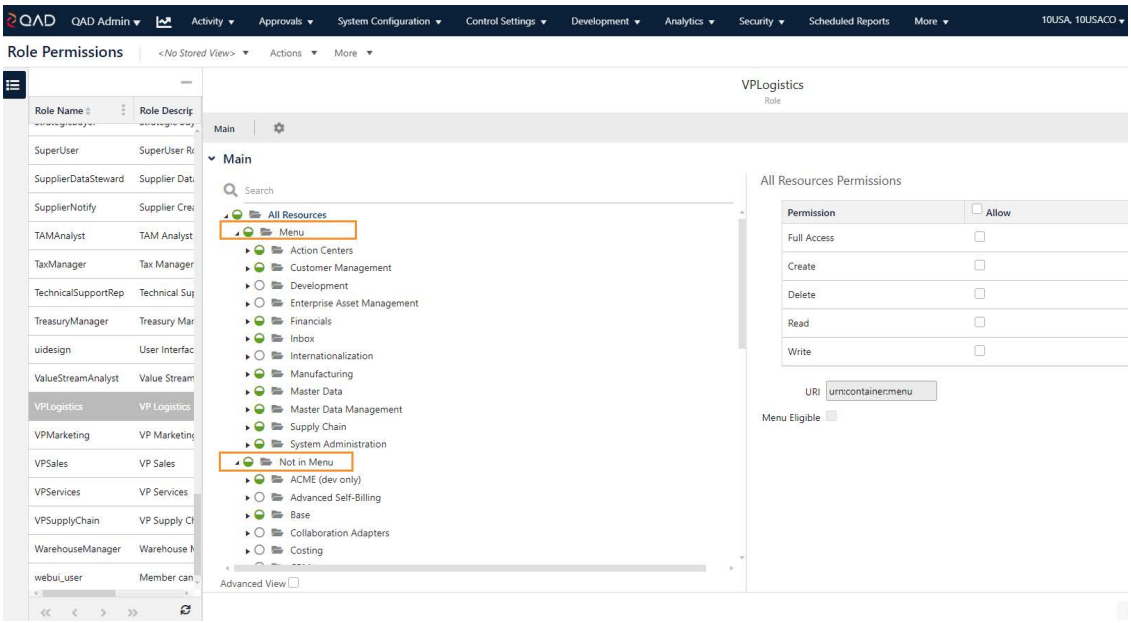
It is recommended to set up and configure permissions for Adaptive UX using role menus and the Permissions option on individual screens. The Role Permissions tree is not intended to be used to set all permissions for a role and should be used sparingly.

Adaptive UX 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 and their permissions cannot be updated on Role Permissions. You can review the default roles' permissions and use these default settings as a guide when assigning permissions to new roles.

Note Use role menus to accurately and efficiently set permissions on new roles. See "Role Menus" on page 129 for more information. See "Fields and Field Groups" on page 151 for information on securing individual fields or field groups.

The main Role Permissions screen displays all the resources that can be secured in the system. In the role permissions tree, the resources are organized by a functional menu structure and are divided into two groups: Menu and Not in Menu, as shown in Figure 7.8.

Fig. 7.8
Role Permissions



The Menu structure contains menu-eligible resources and their dependencies. The menu-eligible resources include the following types:

- Browse-only views

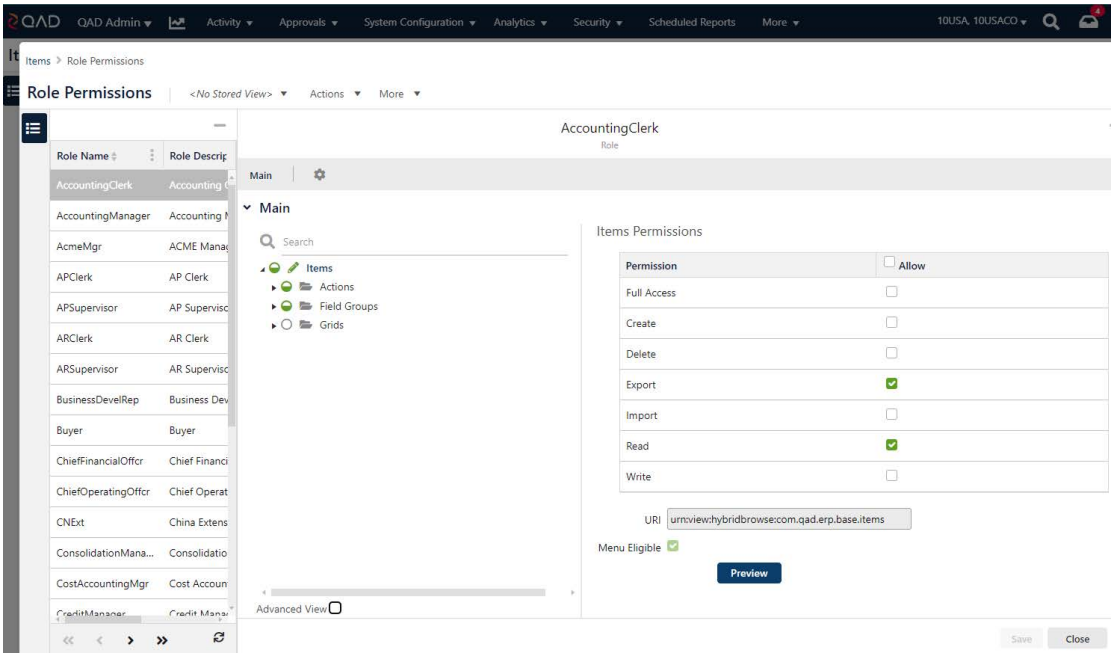
- Hybrid views
- Form-only views
- Reports
- URL links
- Action centers

The Not in Menu structure contains all the remaining resources, as well as the resources of the Menu type that do not display in the Menu structure. The Not in Menu resources include the following types:

- KPIs
- Services
- Scripts
- Views that are used for drill-downs and lookups

Far fewer resources are available to secure in the permissions tree when you select Permissions from the toolbar on an individual screen, such as Item in Figure 7.9. The Role Permissions window shows only the resources associated with that screen, which allows you to secure only the resources that are required for a role to successfully access the associated screen.

Fig. 7.9
Item Permissions



Permission Propagation, Inheritance, and Configuration

Permissions are assigned to views and propagated to the underlying business components and dependent resources.

When you allow Full Access to a view, all dependencies of that view are granted the required permissions. To secure separate parts of a screen, you need to expand the corresponding group of dependencies and set permissions separately by selecting or clearing the checkboxes for the available operations, such as Create, Delete, Read, Write, and so on.

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

Removing Permissions

Removing permissions at the view level does not remove permissions for the dependencies. This secures permissions for the components that are dependencies to other areas of the application. This way the system prevents breaking permissions in other screens.

To clear permissions for a view and its dependencies, select Clear Permissions from Actions in the toolbar.

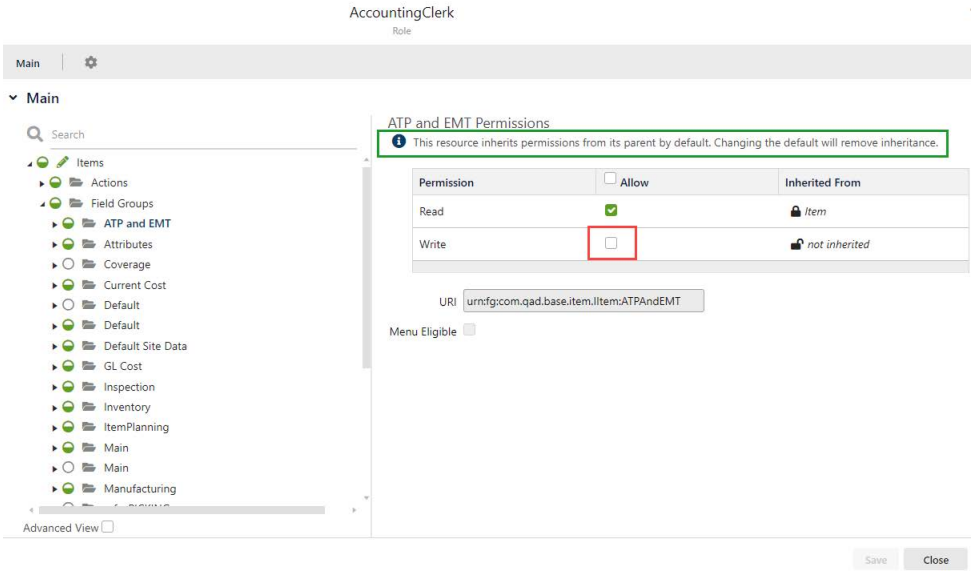
Field Permissions

For field security, permissions are inherited from the parent component, as the owning element. This approach secures the correct permission setup: you cannot allow permissions for a separate field or field group if there are no such permissions for the parent component. Fields and field groups are the only areas of the permission tree that display the Inherited From column to indicate permission inheritance.

To remove any permission for a field or field group, clear the corresponding checkbox in the Allow column, as shown in Figure 7.10.

Note When setting up permissions for fields and field groups, the system displays an information message about the permission inheritance.

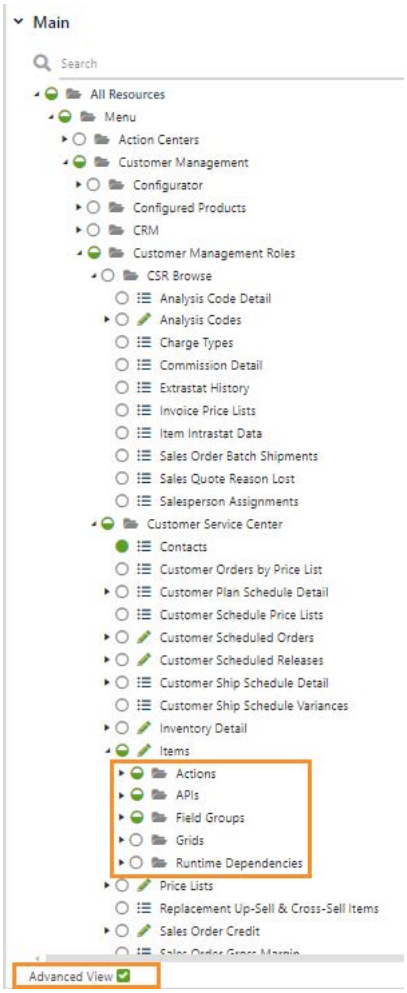
Fig. 7.10
Permission Inheritance for a Field Group



Permission Tree

The permission tree identifies how resources are organized in the system. Resources are arranged in a hierarchy and may have multiple permission types. Figure 7.11 shows the expanded permission tree for the AccountingClerk role.

Fig. 7.11
Role Permissions Tree



A solid green circle represents full access to the operations 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 All Resources is half green, which indicates that the role is granted access to some—but not all—resources in the tree. The role has no access to CSR Browse and partial access to Customer Service Center. The circle next to CSR Browse 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 Customer Service Center is half green, indicating partial access to the resources that make up Customer Service Center. The Customer Service Center resource contains Contacts, which has a solid green circle, indicating full access to the resource.

The permission tree is based on the following structure:

- Views: system resources marked with a green pencil icon
  - Actions: securable actions available in the current view toolbar.
  - APIs: business components and services that make up a screen, including the browse-only portion of a hybrid screen.
  - Field Groups: field groups and securable fields for the current view.

- Grids: external grids available in the current view. For more information about external grids, see “External Grids” on page 149.

Note Internal grids behave as field groups.

- Runtime Dependencies: the runtime dependencies of the current screen; for example, other views triggered by a custom button.

Note APIs and Runtime Dependencies are only visible when you select the Advanced View checkbox.

Permissions Tree Search

You can search for resources by URI or by label name using the Search feature at the top of the permissions hierarchy tree. Search results display the resource type icon to the left of the search list items and partial URIs to the right of the search list items.

Note If you select the Advanced View checkbox, you can search for the business components that are part of the advanced resources, such as APIs or Runtime Dependencies. Otherwise, you can only see the search results based on the resources of the default view.

Fig. 7.12
Permissions Search

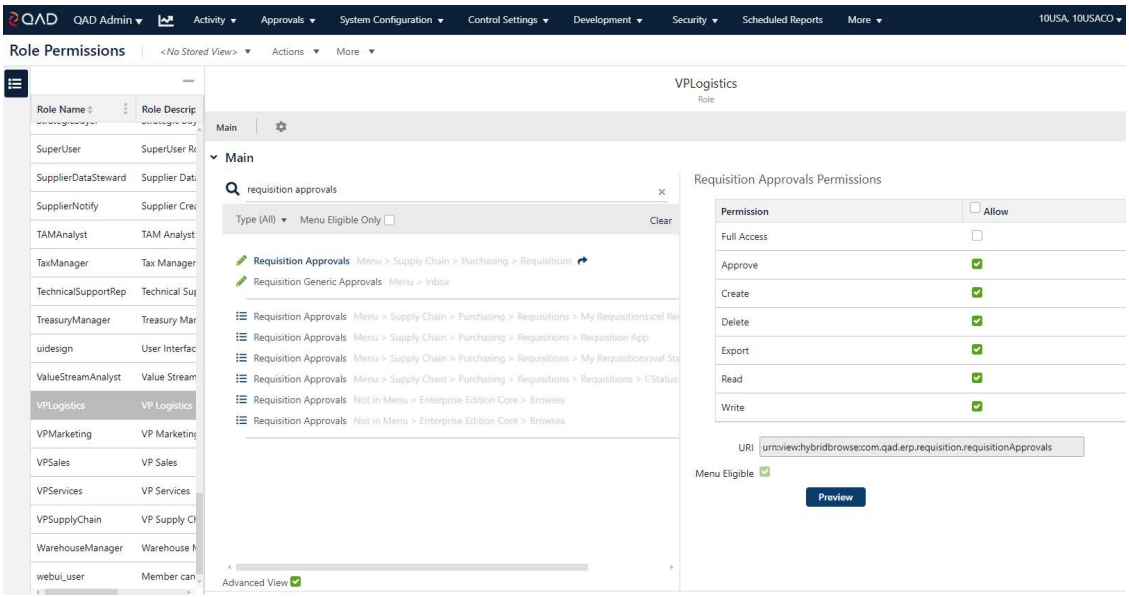
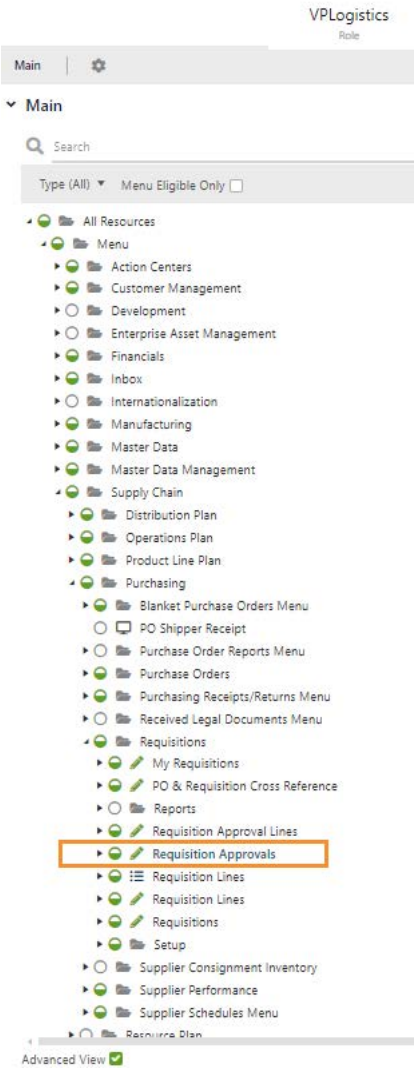


Figure 7.12 shows the search results for requisition approvals for the VP Logistics role. You can click the search result resources to view and update their permissions. If you need more information to determine which of the results is the one you are searching for, you can view each resource within the context of the permission hierarchy by selecting it and clicking the blue arrow next to it.

Fig. 7.13
Expanded View in Context

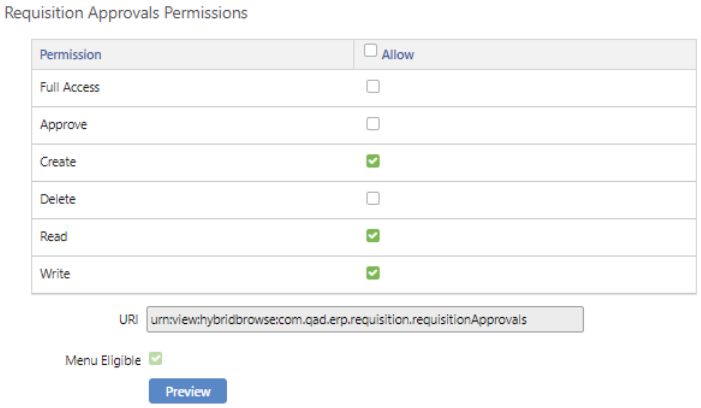


The permission tree expands to show where the resource, in blue, fits into the hierarchy, as shown in Figure 7.13.

Permission Grid

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

Fig. 7.14
Permission Grid



The grid lists the operations for the resource that can be set to Allow.

Note For fields and field groups, the permission grid also contains the Inherited From column. This column indicates if permissions are inherited from any parent business component.

Permission. Full Access, Approve, Create, Delete, Read, and Write operations. Every resource has Read, which allows users of the role to view the data. Full Access allows or denies access to all other permission operations.

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

Note To be able to approve, create, delete, or write, a user's role must have Read access to the resource.

Different resource types have different operations associated with them. Browses, views, and reports have one line in their permissions grids for allowing read access, while business entities have multiple lines that can include approve, create, delete, read, and write.

Below the permissions grid is the resource URI and the Menu Eligible checkbox. This checkbox identifies the resources that can be added to a role menu and found in the Menu Search. It is for informational purposes and cannot be changed.

Resource Dependencies

Resources often depend on other resources to create different elements of Adaptive UX. These dependent entities must be secured for the main resource to have full functionality. The software automatically identifies dependencies and sets permissions as needed.

Whenever you grant role permissions to a specific view, the dependent elements of the permission tree are also granted permissions for this role. Even if you clear the view permissions in the permission grid, it will not propagate to the dependent resources because the system secures the assigned permissions for the dependencies. To clear the permission setup completely for all dependencies and child resources, select the view and click Actions > Clear Permissions.

For example, browses in one business component can be lookups or drill-downs for another business component. For a lookup or drill-down to function correctly, users must have Read permission to the associated browse.

Dependencies appear in the tree grouped by separate containers under a main view: Actions, APIs, Field Groups and Grids. Different views have different sets of the dependency containers, which show all the resources required to populate the main view. However, some of the dependencies do not display in the permission tree structure, because they do not refer to actions, APIs, field groups, or grids. These resources are added as Runtime Dependencies to the business component associated with the view and are granted access automatically whenever it is granted to the parent.

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 that you only see the list of system roles.

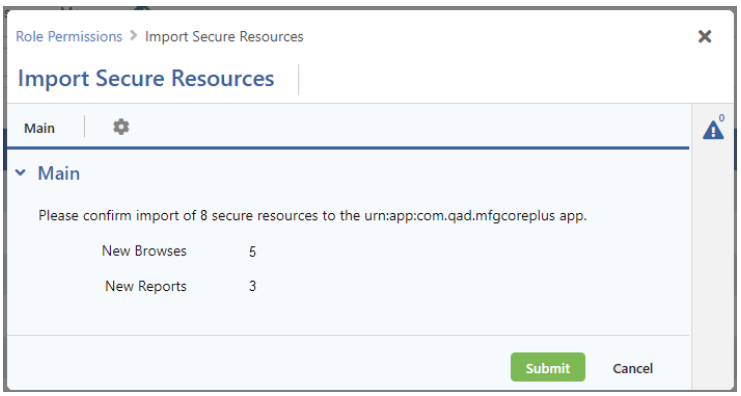
Refresh Permissions

Use the Refresh Permissions action if you make updates to role permissions through Role Permissions Maintain in QAD Adaptive ERP and want the permissions to be updated immediately in Adaptive UX. The action clears all security-related caches and reloads permission data. 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.

Import EE Secure Resources

Use the Import EE Secure Resources action to move browses and QRF reports created in Adaptive ERP into Adaptive UX as secure resources.

Fig. 7.15
Import Secure Resources

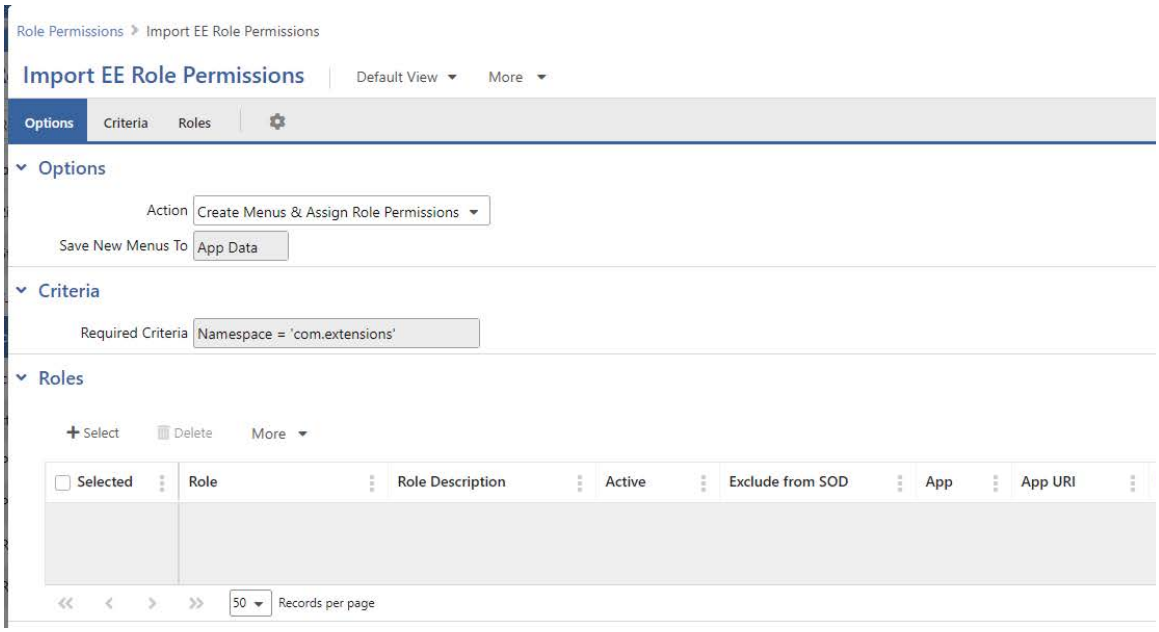


This action displays the Import Secure Resources screen, which lists the number of new browses and new reports that are set to be imported into the defined app. The process creates the secure resources in Adaptive UX, adds them to the cache, and adds them to the ElasticSearch index. The resources are imported as menu-eligible and appear in the Role Permissions tree as individual items.

Import EE Role Permissions

Use the Import EE Role Permissions action to create role menus and role permissions that align with EE role permissions. The action creates a set of menu-eligible resources in top-level folders based on functional area. Those folders become the menu options in the menu bar of Adaptive UX. You can reorganize the menu items and set permissions directly from the Menus screen, or you can choose to have the system set permissions during import.

Fig. 7.16
Import EE Role Permissions



Options

Action. Select one of the options in the drop-down menu.

- **Create Menus & Assign Role Permissions**: (Default) For each selected role, the system assigns EE permissions to the corresponding Adaptive UX permissions, and creates a role menu by functional area for each role from all menu-eligible resources to which the role has permission.
- **Create Menus Only:** The system creates a role menu by functional area from all menu-eligible resources to which the role has permission. The corresponding Adaptive UX permissions are not assigned with this option.

Note If you do not have full access to Role Permissions, the Action field is disabled and set to Create Menus Only.

Save New Menus To. New menus are saved to the same app / app URI as the corresponding role. If the role is stored in Configuration Data, the role's menu is created in Configuration Data. If the role is stored in an app, then the role's menu is created in that same app.

Existing menus are saved to their existing app URI.

Criteria

Required Criteria. Displays the required criteria that are applied to every import of EE resources.

Roles

The Roles panel contains a list of the roles to include in the import. Click the Select link to open a lookup with roles you can import into the current namespace.

Import Options

After you click Submit, the system checks if the selected roles have existing menus and permissions in Adaptive UX. If they do, a window appears with the following choices.

- **Replace**: Overwrites the existing role menu and/or role permissions with the imported settings.
- **Append**: Adds to the existing role menu or role permissions. The action does not overwrite existing settings.
- **Cancel**: Cancels the Submit action and returns you to the Import window.

Assigning Permissions to Roles

Adaptive UX securable resources are listed in the permission tree on Role Permissions. To access and view any of these components in Adaptive UX, a role must have the Allow checkbox selected for the Read operation for the corresponding resources in the Permissions Table.

Note Use role menus and the Permissions option on individual screens to accurately and efficiently set permissions on new roles. See "Role Menus" on page 129 for more information. The Role Permissions tree is not intended to be used to set all permissions for a role and should be used sparingly.

Permission Troubleshooting

If users can log in to Adaptive UX but cannot access screens that you expect them to access based on their role assignments, their role may have missing resource permissions. Use the individual screen's Role Permissions to assign the proper permissions.

1. As the administrator, go to the screen the users cannot access.
2. From the **More** menu, select **Permissions**.

3 Double-click the role that cannot access the screen. The Role Permissions screen appears, displaying only the resources that make up this screen. Assign appropriate access to the operations in the right-hand permission grid.

4 Click **Save** to grant the role the necessary permissions.

Every Adaptive UX screen corresponds to a view resource that is identified with a resource URI. The view may require data from other business components, such as a master screen's subordinate detail screens, lookups, and services. If a user needs access to an Adaptive UX 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 receives 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 153.

You can set up permissions for the following screens and elements in Adaptive UX:

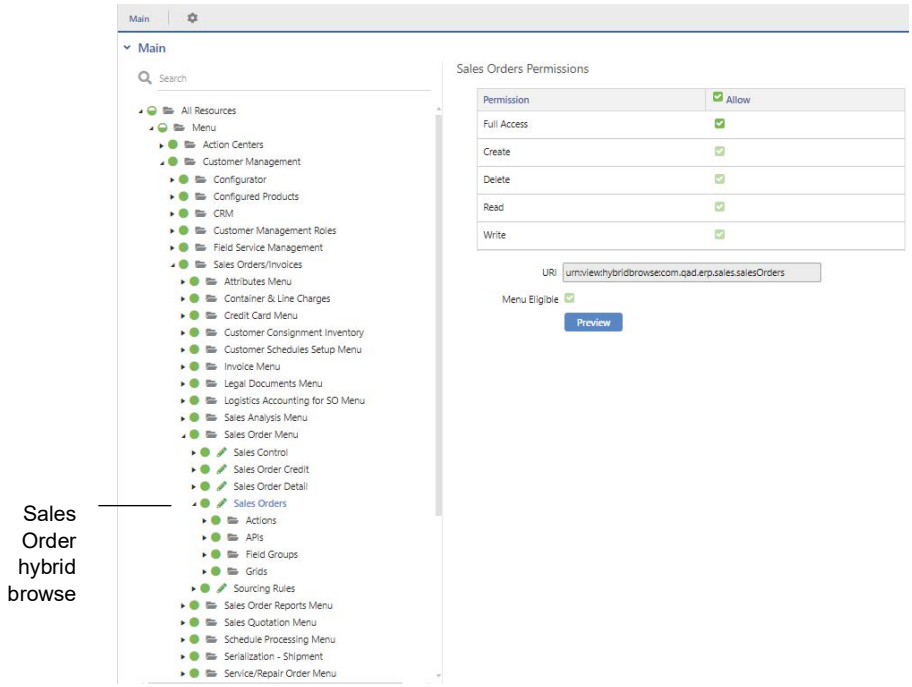
- "Hybrid Browse Screens" on page 147
- "Browse screens" on page 148
- "External Grids" on page 149
- "Lookups and Dashboard Panels" on page 150
- "Fields and Field Groups" on page 151

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 menu containers of the permission tree, as shown in Figure 7.17. The associated actions, APIs, field groups, and grids are collected under the view and can be secured from here.

To configure access to a hybrid browse resource, find it in the Permissions tree and provide the needed permissions.

Fig. 7.17
Hybrid Browse



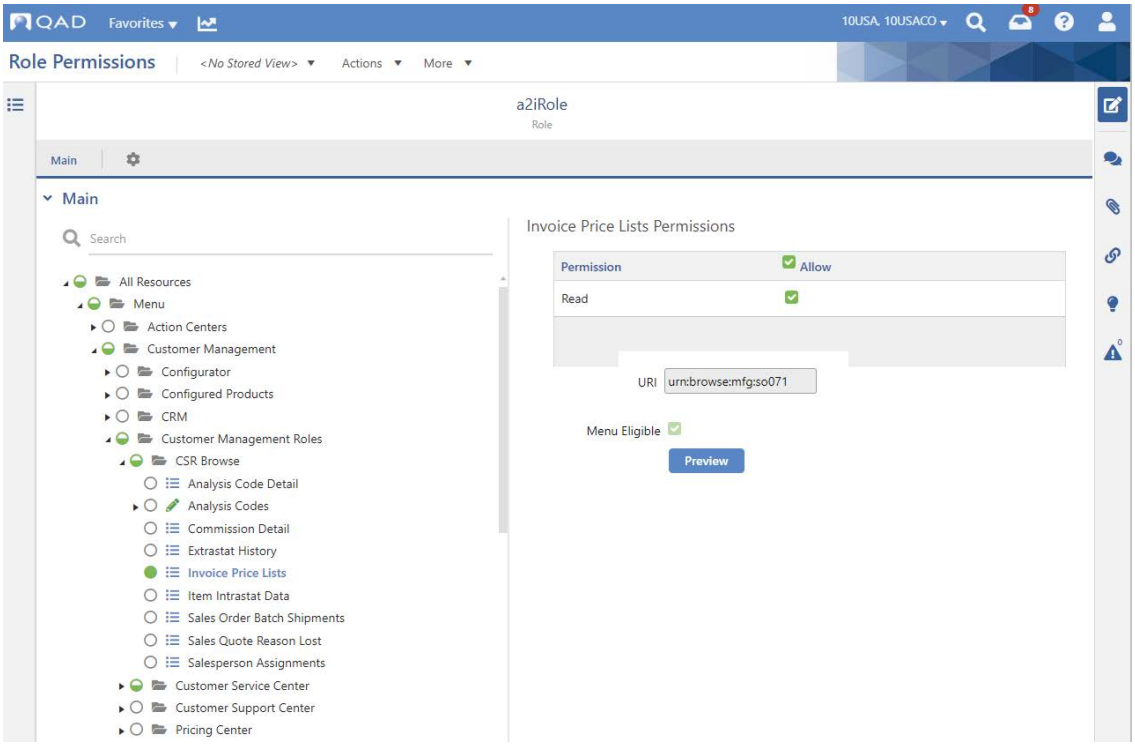
Browse screens

Browses are 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 the associated Browse resource. Permission to the Browse resource gives the user access to the data that loads into the screen.

To configure access, find the associated browse resource in the Permissions tree, as shown in Figure 7.18.

Fig. 7.18
Invoice Price Lists Browse in the Permission Tree



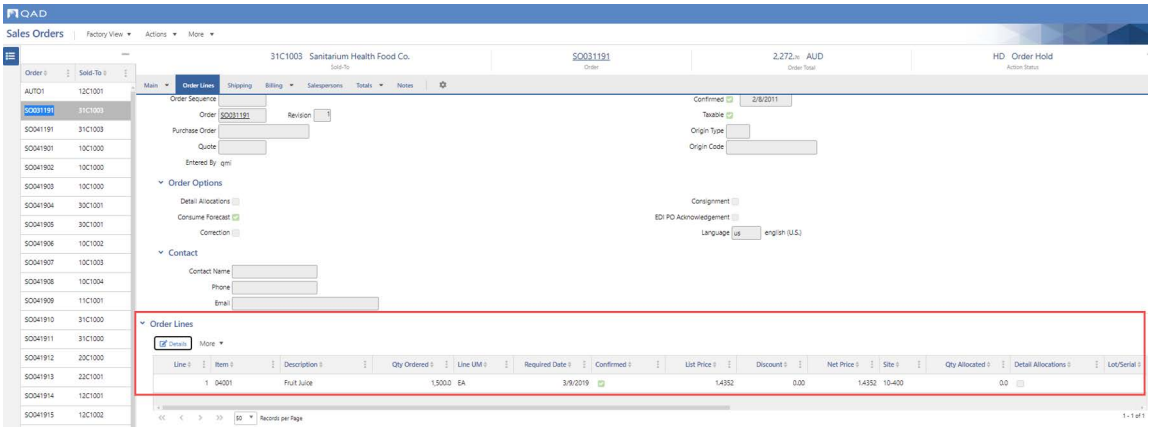
External Grids

Once permissions are set for hybrid browse screens at the view level, some of the screen elements may require additional permission configuration to ensure complete access to all screen elements on the hybrid browse screen. This includes external grids.

External grids have their own hybrid browse screens that require permission configuration. To access these hybrid browse screens, click the Details button available in the external grid.

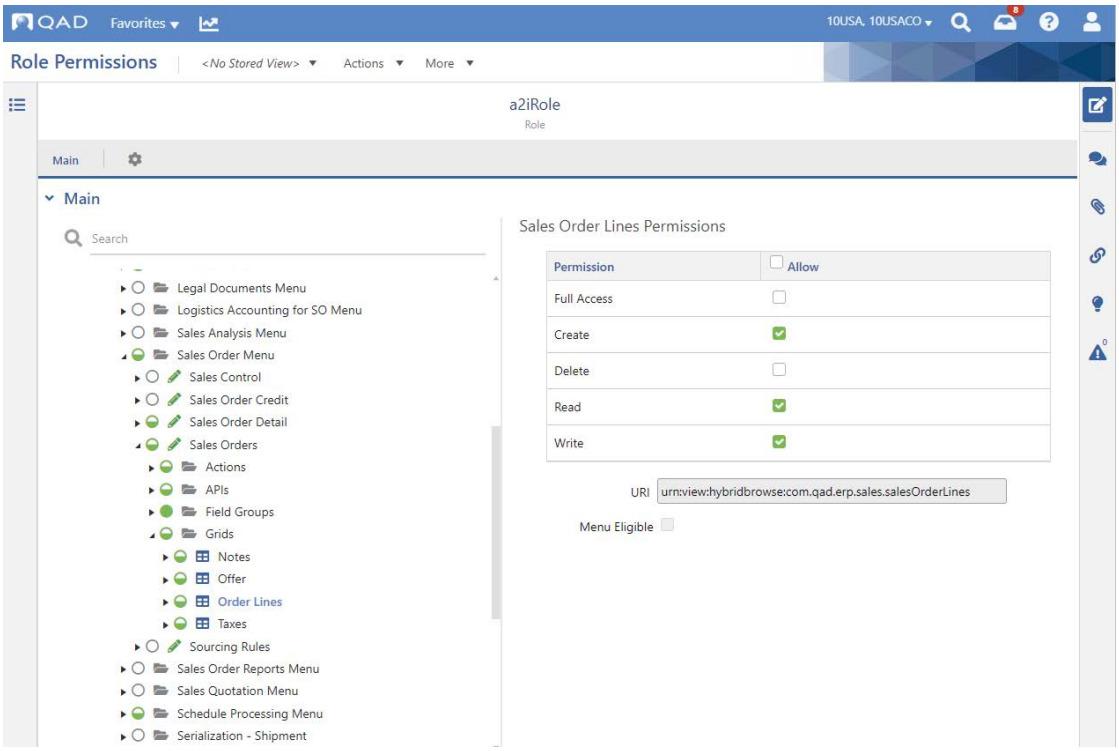
For example, the Order Lines external grid of the Sales Order hybrid browse shown in Figure 7.19 must be secured separately to provide complete access to the screen.

Fig. 7.19
External Grid



To secure an external grid, locate it in the permission tree, as shown in Figure 7.20, and assign corresponding permissions.

Fig. 7.20
Order Lines in the Permission Tree



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 Adaptive UX. With lookups, access is granted automatically if it is granted to the related field. However, if a lookup table is not associated with any field, you must set its permissions to read access.

Otherwise, 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 do not have associated view resources.

Fields and Field Groups

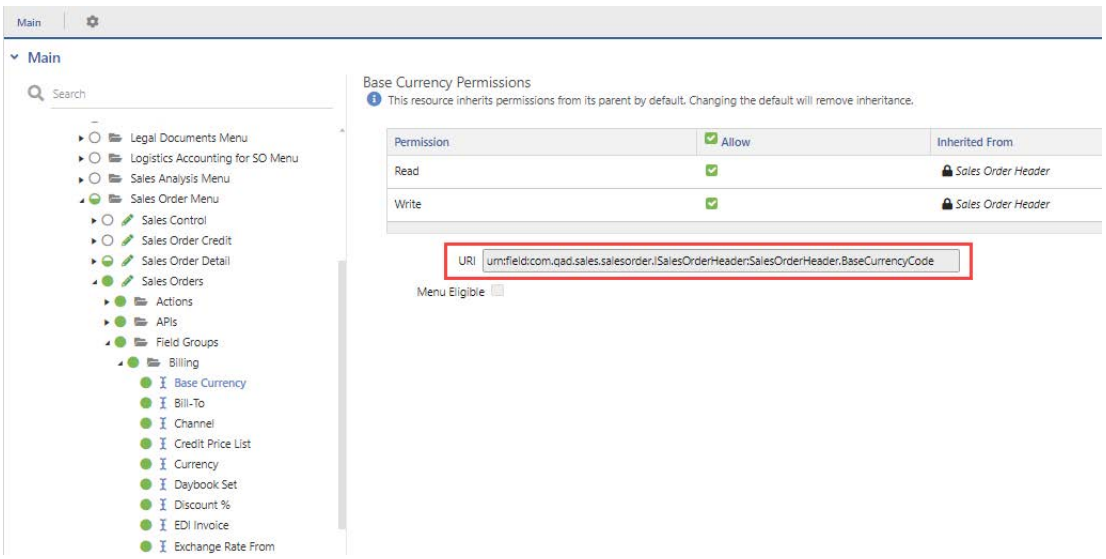
Individual fields and groups of fields are resources that can be secured. Fields and field groups only have read and write permissions. If you determine that more fields in your system need to be secured, contact QAD Services.

Note Since 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.

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 7.21. Fields that are hidden from the screen by field security display with a lock icon in the Configure Panels pop-up.

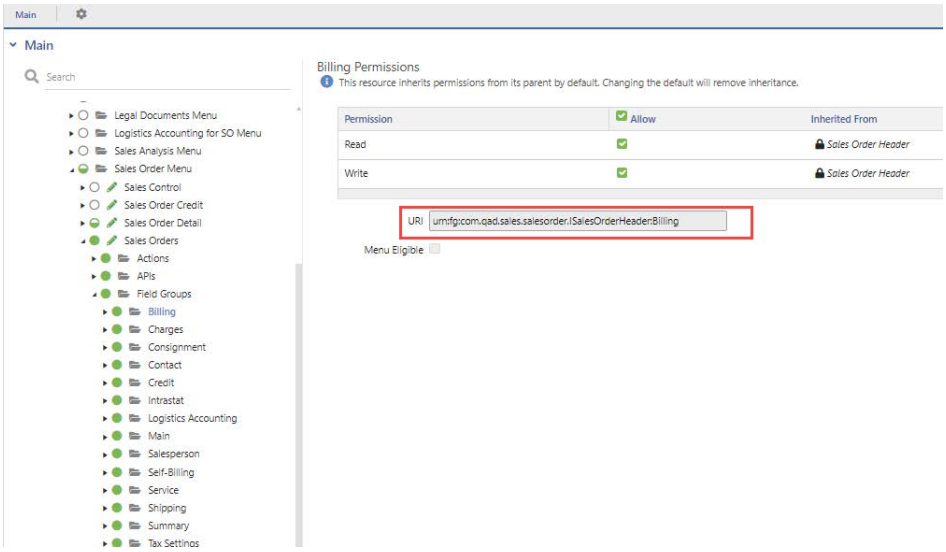
Fig. 7.21
Field Permission



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 *fg* letters, as shown in Figure 7.22.

Fig. 7.22
Field Groups



Securing Fields and Field Groups from Within Adaptive UX

Secure fields and field groups from individual screens containing the fields.

1. Navigate to the screen that requires field security.
2. Select Permissions from the More drop-down in the toolbar to launch the Role Permissions window.
3. Select the role that needs field security enabled.
4. Find the field in the role permissions tree.
5. To make the field read-only, select Allow for the Read checkbox. To remove the field entirely from the screen for this role, clear both the Read and Write checkboxes.
6. Select Save.

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 component that owns the field.

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

FieldName. Name of the field.

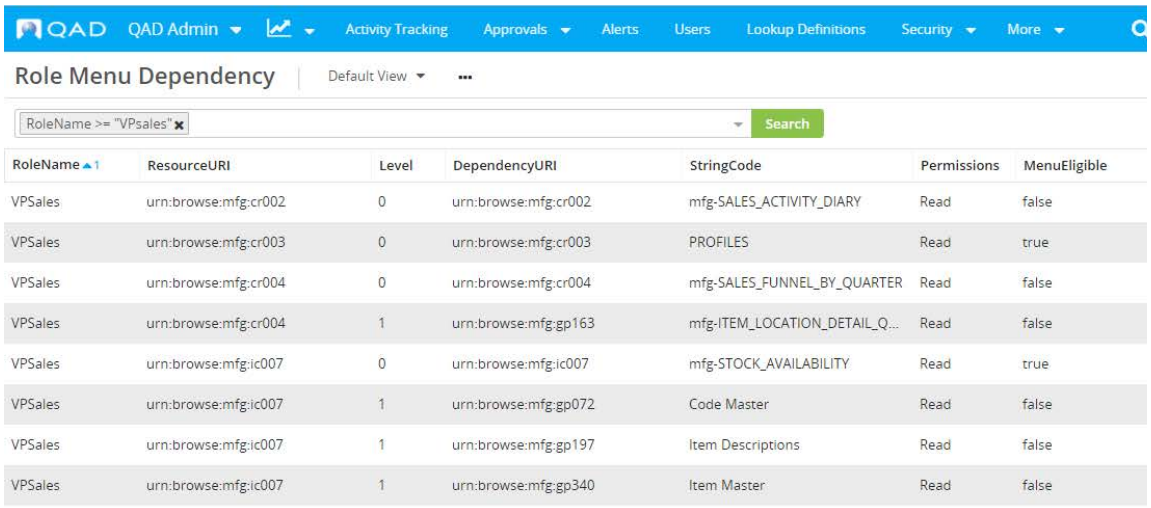
Manually Adding Resources

To add additional secured resources to Adaptive UX, 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. 7.23
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 is not 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 is 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 are not 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.

Troubleshooting Role Permissions

Permissions can be assigned on a screen-by-screen basis, which is effective when users receive 403 errors, indicating a role has not been assigned all necessary permissions. By granting access from the impacted screen, you narrow down the resources to just those required to make the screen functional.

To set permissions for a particular screen:

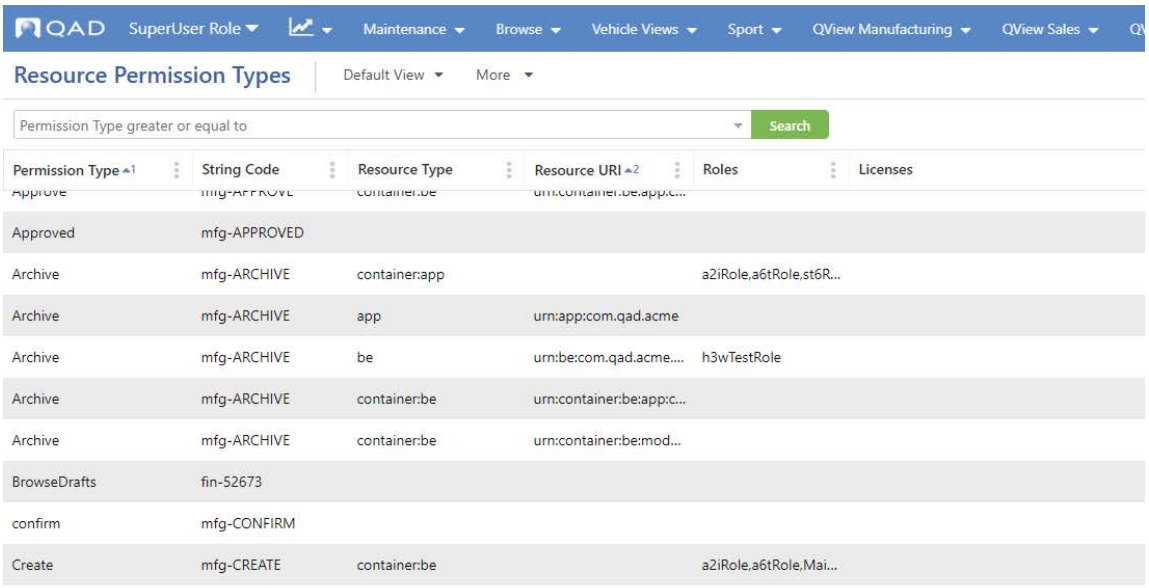
1. Navigate to the screen and select Permissions from the More menu.
2. In Role Permissions, edit the role requiring access.
3. Select Allow in the Permissions Grid for all of the listed resources.
4. Select Save.

If the role continues to receive permission errors, there likely are dependent resources that are not secured. Contact QAD Support for assistance.

Resource Permission Types

The Resource Permission Types browse displays which resources use which permission types.

Fig. 7.24
Resource Permission Types

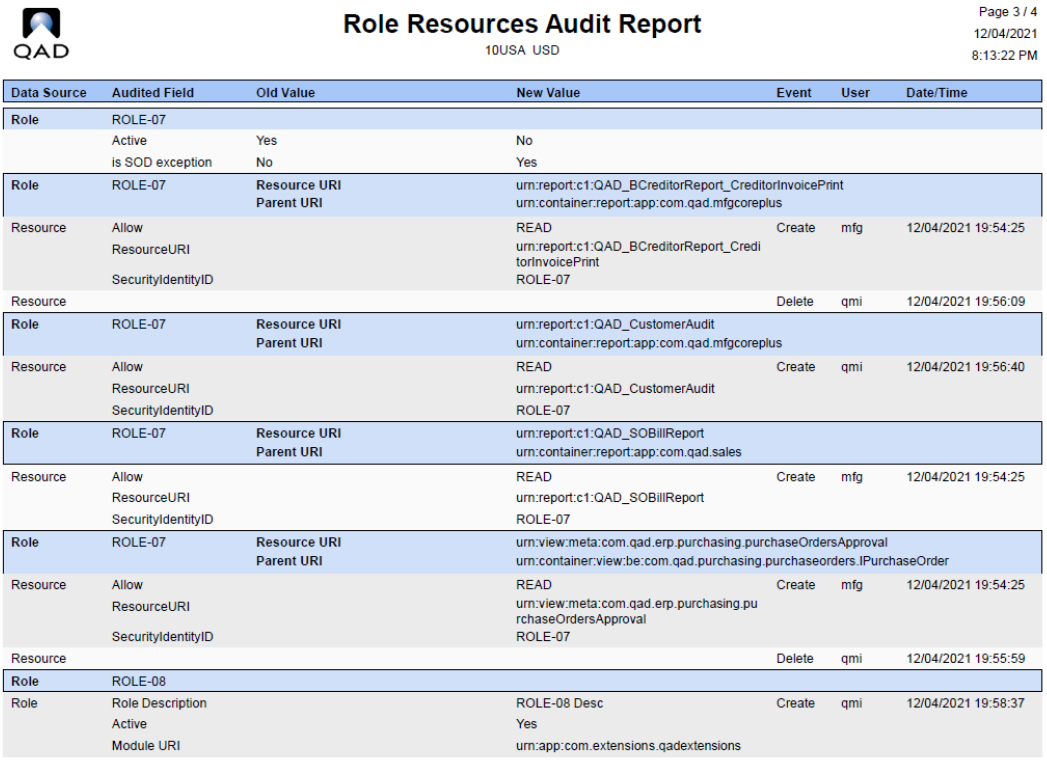


You can use the search functionality to determine which roles or licenses have access control entries for a specific permission type. For example, you can search the Full Access permission type and see all containers and resources that have Full Access assigned. The Resource Type column displays the container type, including individual applications and business components acting as containers because they have child components or services.

Role Resource Audit Report

You can generate the Role Resource Audit Report to review changes made to role permissions for resources in both Adaptive UX and Adaptive ERP. Adaptive UX resources are listed as Resource and Enterprise Edition resources are listed as EE Resource in the report.

Fig. 7.25
Role Resource Audit Report



QAD

Role Resources Audit Report

10USA USD

Page 3 / 4
12/04/2021
8:13:22 PM

Data Source	Audited Field	Old Value	New Value	Event	User	Date/Time
Role	ROLE-07					
	Active	Yes	No			
	is SOD exception	No	Yes			
Role	ROLE-07	**Resource URI**	urn:report:c1:QAD_BCreditorReport_CreditorInvoicePrint			
		Parent URI	urn:container:report:app:com.qad.mfgcoreplus			
Resource	Allow		READ	Create	mfg	12/04/2021 19:54:25
	ResourceURI		urn:report:c1:QAD_BCreditorReport_CreditorInvoicePrint			
	SecurityIdentityID		ROLE-07			
Resource				Delete	qmi	12/04/2021 19:56:09
Role	ROLE-07	**Resource URI**	urn:report:c1:QAD_CustomerAudit			
		Parent URI	urn:container:report:app:com.qad.mfgcoreplus			
Resource	Allow		READ	Create	qmi	12/04/2021 19:56:40
	ResourceURI		urn:report:c1:QAD_CustomerAudit			
	SecurityIdentityID		ROLE-07			
Role	ROLE-07	**Resource URI**	urn:report:c1:QAD_SOBillReport			
		Parent URI	urn:container:report:app:com.qad.sales			
Resource	Allow		READ	Create	mfg	12/04/2021 19:54:25
	ResourceURI		urn:report:c1:QAD_SOBillReport			
	SecurityIdentityID		ROLE-07			
Role	ROLE-07	**Resource URI**	urn:view:meta:com.qad.erp.purchasing.purchaseOrdersApproval			
		Parent URI	urn:container:view:be:com.qad.purchasing.purchaseorders.IPurchaseOrder			
Resource	Allow		READ	Create	mfg	12/04/2021 19:54:25
	ResourceURI		urn:view:meta:com.qad.erp.purchasing.purchaseOrdersApproval			
	SecurityIdentityID		ROLE-07			
Resource				Delete	qmi	12/04/2021 19:55:59
Role	ROLE-08					
Role	Role Description		ROLE-08 Desc	Create	qmi	12/04/2021 19:58:37
	Active		Yes			
	Module URI		urn:app:com.extensions.qadextensions			

The report displays what permissions have been granted to or revoked from the specified resource. If the permissions were newly defined instead of changed, the Old Value column is blank and the New Value column displays the initial record settings.

Fig. 7.26
Role Resource Audit Report - Example

		Parent URI	urn:container:report:app:com.qad.sales	
Resource	Allow		READ	Create
	ResourceURI		urn:report:c1:QAD_SOBillReport	
	SecurityIdentityID		ROLE-07	
Role	ROLE-07	**Resource URI**	urn:view:meta:com.qad.erp.purchasing.purchaseOrdersA	
		Parent URI	urn:container:view:be:com.qad.purchasing.purchaseorde	
Resource	Allow		READ	Create
	ResourceURI		urn:view:meta:com.qad.erp.purchasing.purchaseOrdersApproval	
	SecurityIdentityID		ROLE-07	
Resource				Delete
Role	ROLE-08			
Role	Role Description		ROLE-08 Desc	Create
	Active		Yes	

In Figure 7.26, ROLE-07 was granted read access to the Purchase Orders Approval screen.

For more detailed information on audit trail reports and enabling auditing in your environment, see Chapter 13, “Auditing,” on page 329.

Configure Stored Views Access

You can create and save customized screen layouts, called stored views, in Adaptive UX. These stored views can emphasize important information needed for everyday use and specific tasks by modifying what is visible on the screen, including which columns, fields, and panels are displayed. You can configure different levels of access for the types of stored views a user can create, edit, or delete. The three levels are system, role, and user.

- System Level allows users to create and manage system-wide views that every user who has access to Adaptive UX can view.
- Role Level allows users to create and manage role views that every user assigned to that role can view.
- User Level allows users to create personal views that only they can view and manage. All users have the ability to customize their own views through the webui_user role.

You assign stored views access on Role Permissions. 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. The webui_user role grants all Adaptive UX users the ability to create and maintain personal views, which means you do not need to grant user-level permission to other roles in the system.

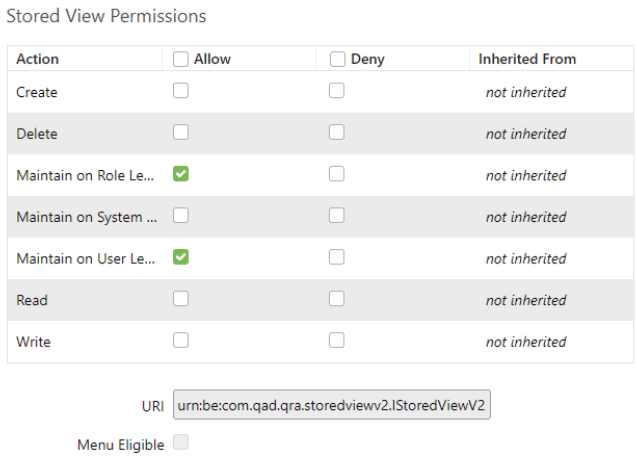
To grant additional stored views permission to a role:

1. Double-click the role on Role Permissions.
2. In the Role Permissions Search menu, enter: **stored view**.
3. Select the result with the URI that ends with IStoredViewV2.

Fig. 7.27
Stored Views Search Result

4. In the permissions grid, select the Allow checkboxes for the appropriate levels and then save.

Fig. 7.28
Stored Views Permission Grid



Note Due to business logic infrastructure, the webui_user role has Create, Delete, Read, and Write access in addition to Maintain on User Level access. Other roles do not need to have these checkboxes selected.

Stored views are created and saved on individual screens within Adaptive UX. Based upon a user's security permissions and the options selected in the Save Stored View As window on an Adaptive UX screen, a stored view can be saved to a single domain or across multiple domains. See the Stored Views entry in the Adaptive UX online help for information on creating stored views.

Record-Level Security

Important Before implementing record-level security, contact QAD to review configuration requirements and evaluate how it will affect your system.

Record-level security allows you to restrict user access to individual records. The Record Level Security browse displays all business components that have record-level security enabled. When record-level security is enabled on a business component, users must be granted access to the records, while the roles to which the users belong must have access to the business component itself. Permission to access a security-enabled record does not grant access to a business component.

Each business component has a resource instance access table. The table contains the groups or users that have access to the business component and their related CRUD permissions. As record-level security is enabled for a business component, the applied security rules do not take effect immediately because the processing of the rules is handled by a batch process that individually updates the tables for each instance of a component.

Important If you enable record-level security in Adaptive UX for business components that access data also displayed in QAD Adaptive ERP browses, you must remove those legacy browses in Adaptive ERP. Adaptive ERP does not support record-level security and users will be able to access secure records to which they have not been granted permission.

Configuring Security Rule Properties

The following YAB properties control security rule record processing:

Table 7.1
Elasticsearch Properties Configuration

Property	Default Value	Description
qad-qracore.securityrules.processing.enabled	false	Determines if security rules are automatically updated in the system.Set to *true* to enable security rule batch processing.
qad-qracore.securityrules.processing.delay.seconds	900 seconds (15 minutes)	Controls how often batches of new or modified security rule records are processed in the system.
qad-qracore.securityrules.processing.threadpool.size	5	Controls the maximum number of parallel threads that can be used to apply security rules for each record.
qad-qracore.securityrules.processing.batchSize	1000	Determines how many records are fetched with each batch.

Before you start working with record-level security within the Adaptive UX, set the `qad-qracore.securityrules.processing.enabled` property to *true* in the `build/config/configuration.properties` file. This enables batch processing of your security rule records as you create and update them. Adjust other settings as necessary for your implementation. After you update the `configuration.properties` file, run the following command:

```
yab webapp-webshell-config-content-update
```

```
yab tomcat-webui-restart
```

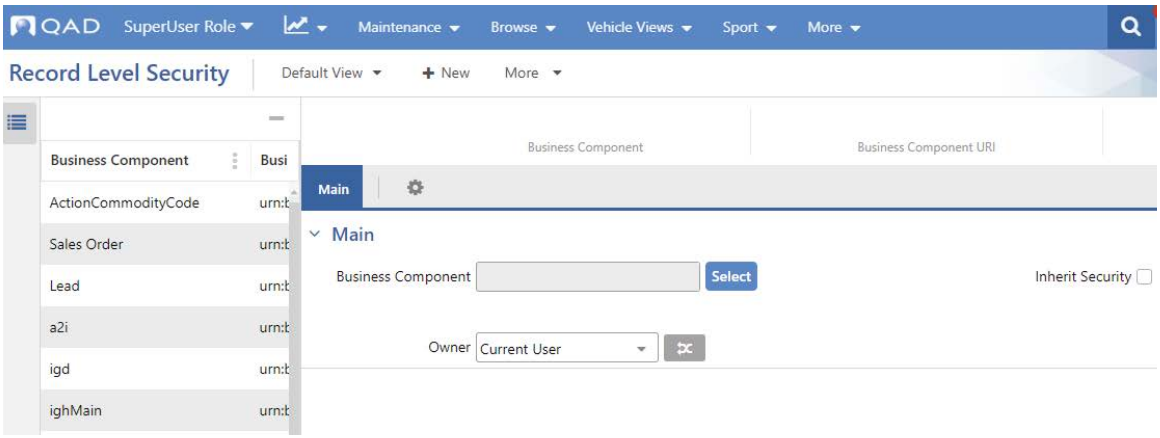
Enabling Record-Level Security

It is important to remember that when you enable record-level security on a business component, access is immediately restricted to the business component's records. Initially, the only users who can view the business component's records are the owners

and the users who are assigned to the Administrator Role defined in Security Control. You must share records with other users, through any of the methods described in “Granting Access to Records” on page 161, before other users can view or edit secure records.

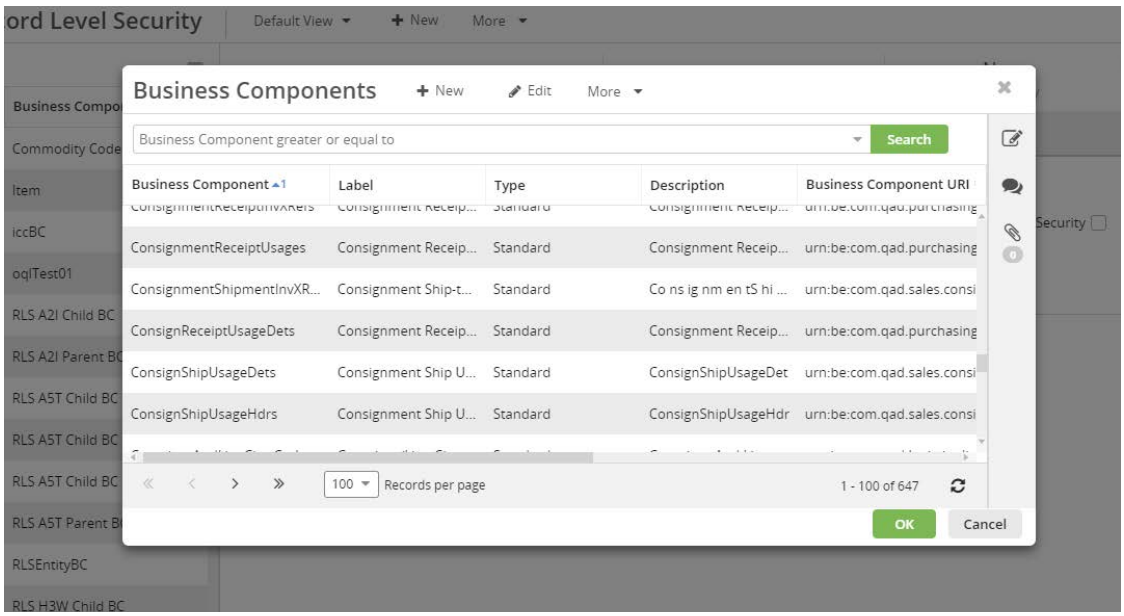
1 To enable record-level security for a business component, select New on the Record Level Security browse.

Fig. 7.29
Record Level Security



2 Select the business component from the lookup.

Fig. 7.30
Business Component Selection



3 Select the owner for the business component’s existing records. The owner can be a single user ID or a dynamic, non-literal owner chosen from the drop-down menu. Use the toggle button to switch between options. The dynamic options available in the menu are all of the character-8 fields on the selected business component. When you select a dynamic option from the menu, the system checks to see if the value of the selected field matches a user in the user table. If a user is found in the table, that user

becomes the owner. If the field is blank or the value does not match a user, the current user securing the records is assigned ownership. You can view the owners of all secured records on the Secure Records browse.

4 If this business component should inherit its record-level security from another business component, select the Inherit Security checkbox, then select the parent business component from the Inherited From lookup.

Note The parent-child business component relationship must already be established to use this functionality. Set up business component relationships in the Relationship panel of Business Components.

5 Select Save.

Granting Access to Records

You can grant users access to secure records in three ways.

1 Manually sharing

2 Automatically using security rules

3 APIs

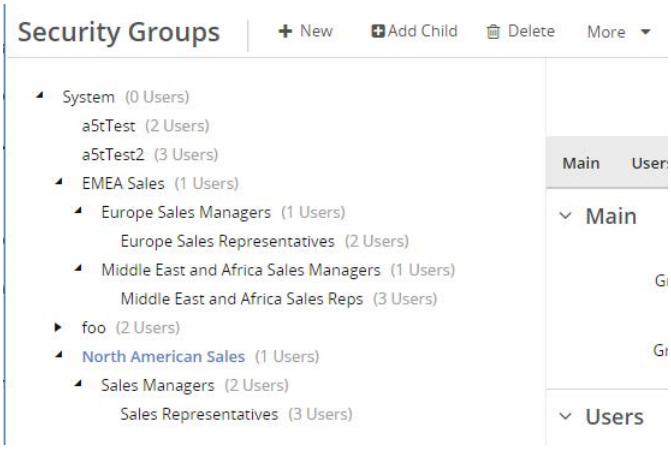
Security Groups

Security groups organize groups of users. You can use these groups to share records with all three sharing methods. All security groups belong to a single hierarchical structure. This structure is displayed on the left side of the Security Groups screen. The right side displays the specific information for the security group selected in the tree.

Using the Tree and Toolbar

The tree is arranged alphabetically and cannot be reorganized. Each item in the tree displays the group's Group Label, number of users assigned to the group, and a toggle icon to indicate if the element has child groups associated with it. Members of a parent group are not automatically members of associated child groups. For example, in Figure 7.31, the VP of Sales is a member of the North American Sales group, but is not a member of the North American Sales Representatives group, because the organization decided the VP of Sales does not require access to all of the sales representatives' records.

Fig. 7.31
Security Groups Tree and Toolbar



The tree structure is primarily controlled by the toolbar. Use the toolbar to create and delete groups.

New

Adds a sibling to the selected tree item. You cannot add a new item when the top node is selected.

Add Child

Adds a new child item to the currently selected tree item.

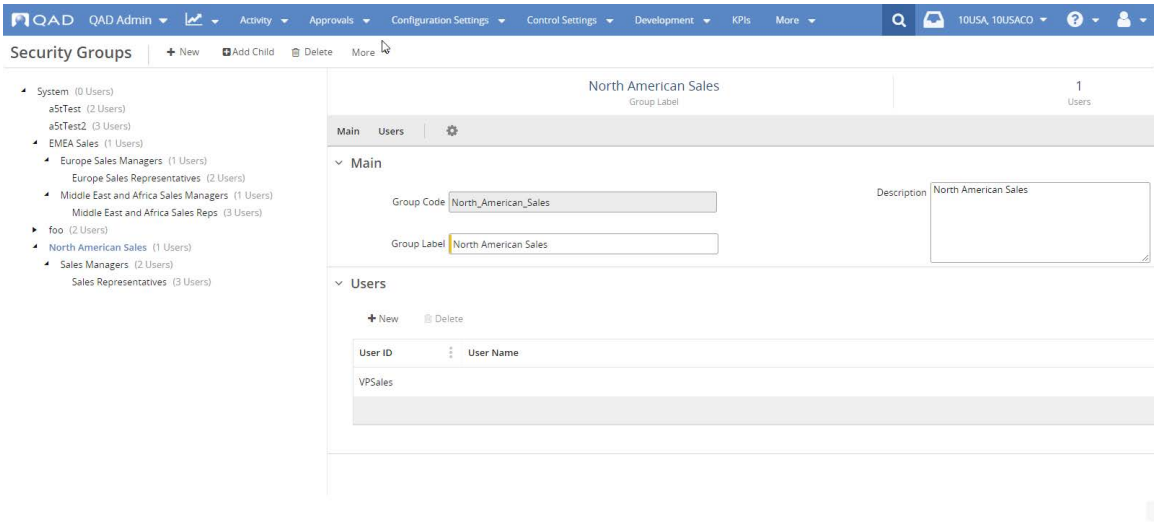
Delete

Removes the selected item from the hierarchical tree view.

Viewing Group Details

The right side of the Security Groups screen displays the group information, including the users assigned to this group.You can update the group's display name, description, and members.

Fig. 7.32
Security Groups Main Panel



Main

The Main panel contains the following sections. Enter the Group Code when creating a new group or a child group.

Group Code. The coded name for the group. This code must begin with a letter and be two to 32 characters in length. It can contain letters (a-z and A-Z), numbers (0-9), and the underscore character. It cannot contain spaces.

Group Label. A label for the group, which displays in the tree and at the top of the Security Groups form. This label can be translated.

Description. A text field for a plain-text description of the group.

Users

The Users grid lists the users who are part of the selected group. To add a user, select New. Then select a User ID from the lookup and select Save. To remove a user from the group, select the User ID in the Users grid and then select Delete.

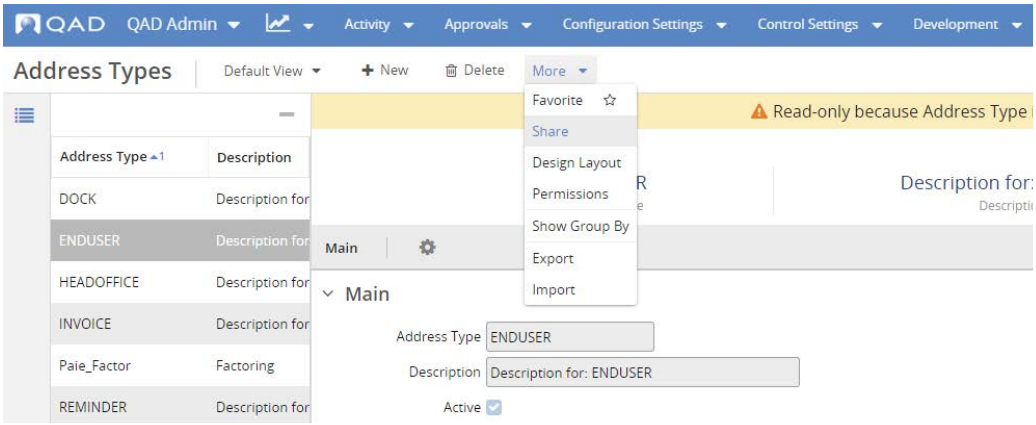
Note Level of access is always set at the role level, so even if a user is in a security group that has access to a record, if that user's role does not have access to the record's business component, the user cannot access the record.

Manual Sharing

Every secure record has an owner. This owner and other users with adequate access can grant other users access to a record by sharing the record from the individual business component's hybrid view.

1. Double-click the record you want to share.
2. Select Share from the More drop-down menu.

Fig. 7.33
Share Access



3 In the Share screen, first select the type of user who should have access to the record. You can choose Everyone, User, or Group if security groups have been set up in the system.

4 Using the lookup in the Name column, select the individual user name or group name.

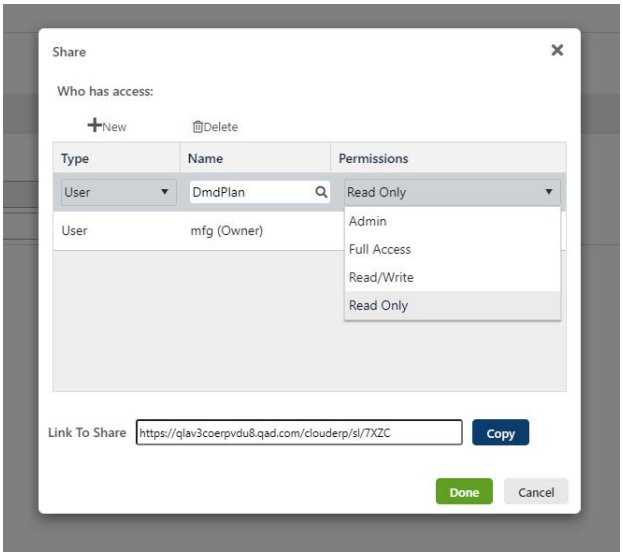
When Everyone is selected as the Type, the Name column is disabled. All users with access to the business component can access the record.

5 Select how much access the user should have. The permission levels you can select are:

- Read Only
- Read/Write
- Full Access
- Admin

Note Admin permission provides full access plus the ability to change the ownership of a record, as long as the Owner field for the business component is set as Current User in Record Level Security.

Fig. 7.34
Define Share Access



6 Select Done to grant access.

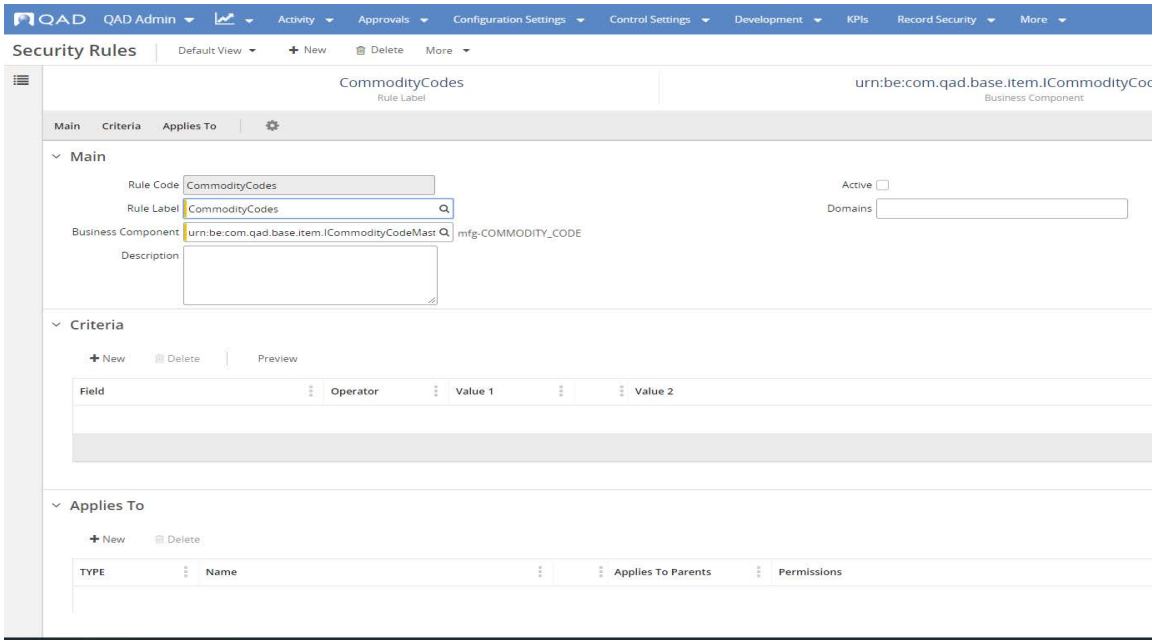
Note Users do not receive notification that they now have access to this record. This functionality is planned for a future release. Consider copying the Link to Share and sending the short link to the users who have received access.

Automatic Sharing with Security Rules

You can automate sharing using security rules, which filter and apply record-level security permissions against record-level security enabled business components. When record-level security is enabled on a business component, users require access to the component itself through their roles, defined in Role Permissions, and to the specific instance of a record. Granting access to records does not happen immediately upon save when using security rules unless you use the action Reapply Security Rules. The rules are applied through batch processing and it can take some time with large datasets for the new permissions to take effect. You can view the status of submitted requests on the Secure Records and Secure Record Detail browses in the Processed column. Requests that have been saved but not activated display No in the Processed column, while those that are active in the system display Yes.

Defining New Security Rules

Fig. 7.35
Security Rules



Main

Rule Code. The coded name for the rule. This code must begin with a letter and be two to 32 characters in length. It can contain letters (a-z and A-Z), numbers (0-9), and the special characters # $ _ % &. It cannot contain spaces.

Rule Label. The label for the rule, which displays at the top of the Security Rules form. This field supports translatable strings.

Business Component. The business component to which this rule applies. The lookup only displays record-level security enabled business components that do not inherit their record-level security from another component.

Description. A text field for a plain-text description of the rule.

Active. A checkbox that determines if the rule is in effect. Until the Active box is selected, the rule does not take effect, even upon save.

Scope. A dynamic text field that supports comma-separated values for restricting the scope of a rule. This field label varies, depending on the business component selected from the lookup. You cannot define scope for a system-level business component. All other business components can be limited in scope based on their system level, from domain, to entity, to site. If no information is entered in the field, the rule is not limited at the defined system level.

Criteria

This grid filters records from the selected business component based on the selected criteria. The rules for combination of conditions are standard. Criteria with different fields are joined with an AND operation. Lines that have the same field code are joined with an OR operation.

Field. The field that is evaluated in the rule. The drop-down menu contains:

- The selected business component's fields.
- Fields from the Instance Security Access Table, which includes fields such as Owner.
- Fields from business components that have relationships with the selected business component as defined on the Business Components screen. This also includes fields from the related business components' Instance Security Access Tables.

Operator. A drop-down menu with operators. Custom operators can appear in this menu, based on the specified field. For example, Member Of is available when the Field column is Owner.

Value 1. The item that is being compared against the field value defined in the Field column. The type of this field varies based on the Field and Operator. For example:

- A numeric Field value shows a numeric input field for Value 1.
- A boolean Field value shows a drop-down menu with yes or no options.
- A user Field value along with a Member Of custom operator shows a lookup of groups.
- A user Field value without a Member Of operator shows a lookup of users.

You can switch the contents of the Value 1 field by selecting the toggle button directly to the right of the field. This switches the field from its initial state into a drop-down menu with variable selections. The selections are fully qualified fields from the selected business component and related business components that match the data type of the field in the Field column.

Value 2. The second value for range function. This field is only active when Value 1 is a range type.

Preview

The Preview option in the Criteria toolbar displays all the records that match the criteria you entered in the grid. You cannot edit the record information, but it helps you determine if you are defining the criteria in the way you intended.

Applies To

Type. User or Group.

Name. The user name or user group to whom the rule applies. When User is selected in the Type field, you can toggle the Name field between a lookup of the Users browse and a drop-down menu of the user fields from this and related business components.

Permissions . Select how much access the user or group should have. The permission levels you can select are:

- Read Only
- Read/Write
- Full Access
- Admin

Applies To Parents. Yes or No. Active when Group is the selected type. Determines if the permissions for a security group are applied to the group's parents. A child group can have permissions separate from and greater than the parent's.

APIs

You can use the Business Logic API to share records with users. Contact QAD for detailed information on implementing this sharing method.

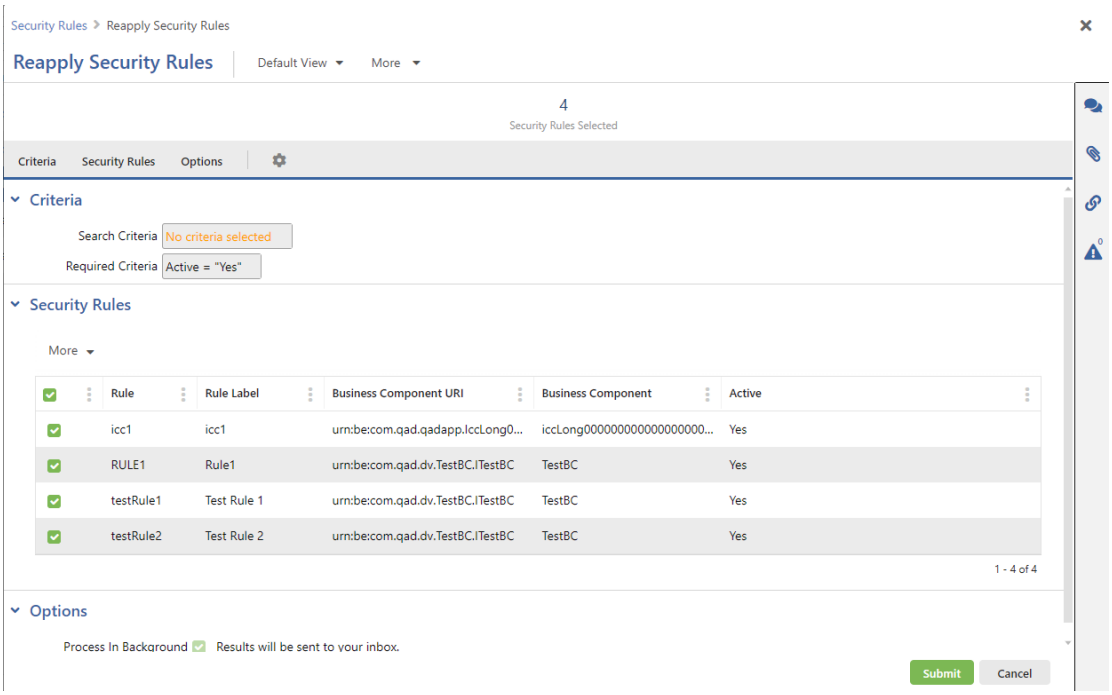
Reapply Security Rules

New record-level security rules are applied at regular intervals, but if needed, you can use this action to update the access provided by the security rules immediately. The process deletes existing access grants if the security rule no longer provides them and creates new access grants according to the Search Criteria and selected rules in the Security Rules grid.

Note Access provided by the Share feature is not impacted by the Reapply Security Rules process.

Reapplying these rules can put a heavy load on the system and it is recommended that you ensure you have completed all changes before applying an update.

Fig. 7.36
Reapply Security Rules



Criteria

Search Criteria. The search criteria defined in the Security Rules browse. If no search criteria were specified, this field displays “No Criteria Selected.”

Required Criteria. This field is always set to Active=Yes. The Reapply Security Rules screen only displays active rules, with inactive rules automatically filtered out.

Security Rules

The Security Rules grid displays the system's active security rules and selects them all by default when the window opens. You can clear rules that do not need to be updated immediately.

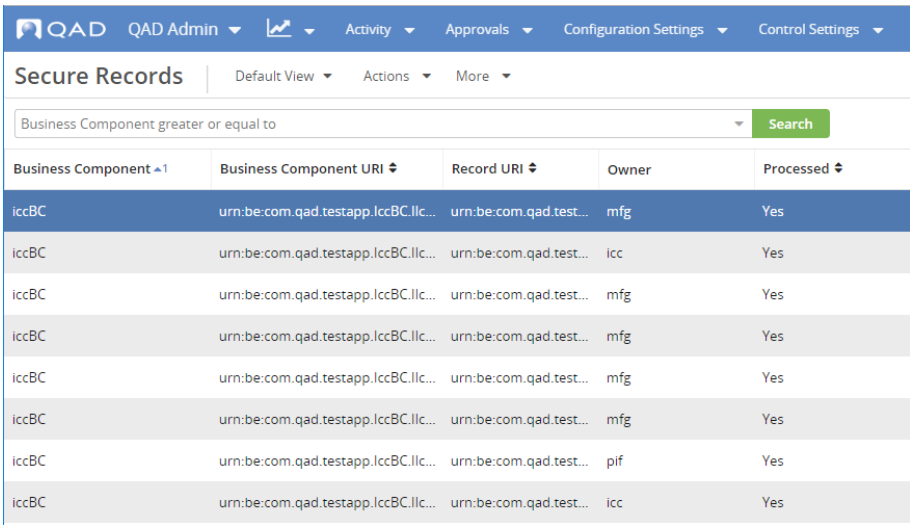
Options

The process of reapplying security rules always runs in the background. The Process in Background checkbox cannot be cleared.

Secure Records Browse

The Secure Records browse lists one entry for each record that is secured in the system. The entry identifies the business component label and URI, record URI, owner, and if the record has been processed.

Fig. 7.37
Secure Records



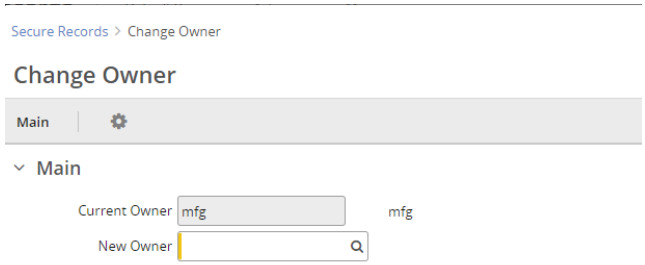
Use this browse to change the ownership of secure records, either as an individual or bulk action. This is useful if an employee leaves the company and you want to reassign all of that user's records to a new user.

Change Record Ownership

To change the owner of an individual record, select the record in the browse and choose Individual Change Owner from the Actions menu.

Note Individual owners of records do not require administrator rights to transfer their own records to other users. The owner can go to the business component, highlight the record, and then select Change Owner from the More menu.

Fig. 7.38
Individual Change Owner



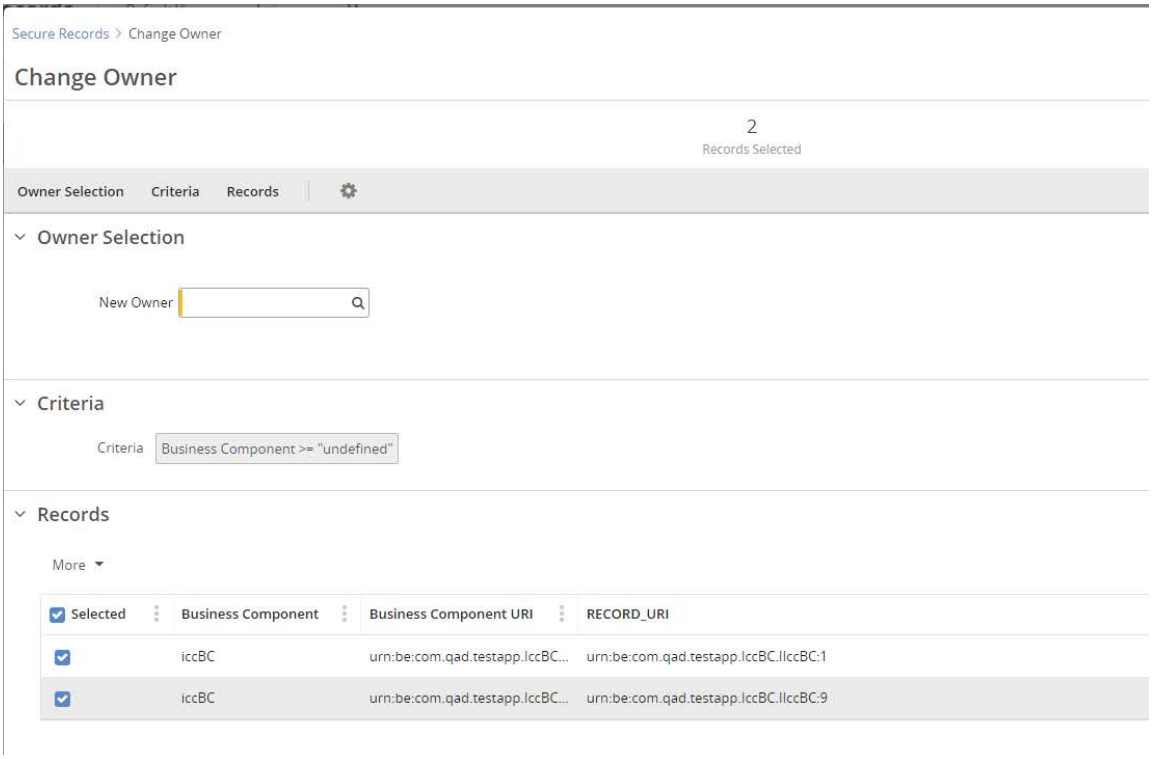
Choose the new owner from the New Owner lookup and then select Submit. The new owner now has full access to the record. It is important to remember that the previous owner no longer can access the record unless that user has been granted access through any method of sharing.

Bulk Ownership Change

To change the owner of multiple records at once:

1. Use the Search box to build criteria for filtering. For example, if you are reassigning all records owned by one user to another user, filter by the current owner's user ID.
2. From the Actions drop-down, choose the bulk Change Owner.
3. In Change Owner, choose the user ID of the new owner and check that all records listed in the Records panel should be reassigned. Clear any records that should not be assigned to the new owner.

Fig. 7.39
Bulk Change Owner

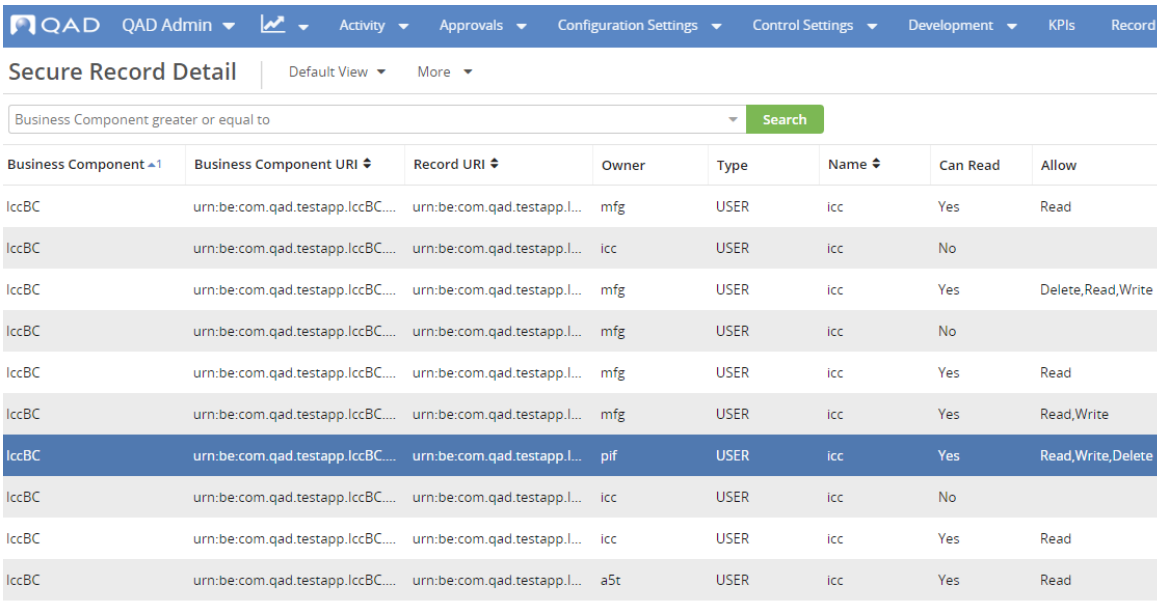


4. Select Submit to save.

Secure Record Detail

The Secure Record Detail browse is more granular than the Secure Records browse. While the Secure Records browse lists every record that is secured in the system, the Secure Record Detail browse lists every user who has access to each record and what level of access the user has.

Fig. 7.40
Secure Record Detail Browse



Chapter 8

QAD Adaptive ERP Security

This section discusses how to set up additional types of security specific to the QAD Adaptive ERP.

SSH on the QAD Adaptive ERP 174
Describes the settings for SSH.

Public Key Authentication for SSH 175
Explains how to set up public key authentication.

SSH for QAD Adaptive ERP Terminal Mode 177
Explains the safeguards of using SSH instead of telnet.

HTTPS for QAD Adaptive ERP Desktop Screen Display 177
Explains how to set up HTTPS for QAD Adaptive ERP Desktop screen display.

HTTPS for AIA 178
Describes how to set up AppServer Internet Adapter (AIA) with HTTPS.

SSL for AppServerS and AppServerDCS 179
Describes how to configure SSL for AppServerS or AppServerDCS.

Additional Security for Standard Programs 181
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 Adaptive ERP

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 175, 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 175, enter the passphrase.

Public Key Authentication for SSH

SSH supports both password-based authentication and public key authentication. By default, the QAD Adaptive ERP 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+MUzdm99CdneN0fQHEjvTxtyBCvyUx+dotKOl0DuCteMHsASuyTW
   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 Adaptive ERP Terminal Mode

For QAD Adaptive ERP 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 Adaptive ERP 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 Adaptive ERP terminal mode are included in the “SSH and Telnet Protocols” appendix of the *QAD Enterprise Edition Installation Guide*.

HTTPS for QAD Adaptive ERP Desktop Screen Display

In the QAD Adaptive ERP, 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 Adaptive ERP. However, instead of using HTTP, you can use HTTPS.

To set up HTTPS for QAD Adaptive ERP Desktop screen display:

1. Enable the SSL Connector in Tomcat. See page 40.
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.

SSL for AppServerS and AppServerDCS

This section describes the steps required to enable SSL for AppServerS and AppServerDCS, specifically to secure the AppServer connections to the QAD Adaptive ERP client. It is recommended that you read through all of the steps before beginning the process. Contact QAD Services for assistance.

The examples in this section may differ from your environment due to the configuration used when the necessary security certificates for Java and OpenEdge were set up.

1 Complete the first four steps described in the Progress Knowledgebase article "How to Enable SSL for Webspeed and or/AppServer."

https://knowledgebase.progress.com/articles/Article/P109432

Make note of the key alias name you give the certificate upon import because you will need it later.

For more details from Progress, see SSL-enabled AppServer and SSL-enabled AppServer operation.

2 Use the `genpassword` utility to obtain the key alias password, required for step 5.

```
proenv> genpassword -password
```

3 Determine what AppServers are part of your system. Enter:

```
yab -instance config appserver
```

You should see a result similar to the following:

```
appserver.fin
appserver.mfg
appserver.eam
appserver.crm
appserver.qra
appserver.qxosi
appserver.qxoui
appserver.qxtnative
```

Depending on your system configuration, you must secure two or three AppServers. All configurations must secure `fin` and `mfg`. If EAM is installed and in use, you also must secure the `eam` AppServer.

4 Use the config command to determine the URLs of the AppServers you are going to secure. Enter:

```
yab config appserver.xxx.url
```

where xxx is the AppServer abbreviation. For example, to determine the URL for the `mfg` AppServer, enter:

```
yab config appserver.mfg.url
```

The command returns a URL similar to:

```
appserver.mfg.url=appserverdc://server.domain.com:22064/as-mfg
```

This URL is required for step 5.

5 In the `configuration.properties` file, add the following information, replacing `xxx` with the appropriate AppServer abbreviation. Also, when entering the AppServer URL, edit the line by adding an ‘s’ to `=appserverdc` so that it reads `=appserverdcs`.

```
# Adding Appserver SSL configuration
appserver.xxx.sslenable=1
appserver.xxx.keyalias=
appserver.xxx.keyaliaspasswd=

appserver.xxx.url=appserverdcs://URL returned in step 4/as-xxx
```

For example, to enable SSL on the AppServers required to secure the Adaptive ERP client connections, add:

```
# Adding Appserver SSL configuration
appserver.mfg.sslenable=1
appserver.mfg.keyalias=key alias name from step 1
appserver.mfg.keyaliaspasswd=key password from step 2
appserver.mfg.url=appserverdcs://URL returned in step 4/as-mfg

appserver.fin.sslenable=1
appserver.fin.keyalias=key alias name from step 1
appserver.fin.keyaliaspasswd=key password from step 2
appserver.fin.url=appserverdcs://URL returned in step 4/as-fin

appserver.eam.sslenable=1
appserver.eam.keyalias=key alias name from step 1
appserver.eam.keyaliaspasswd=key password from step 2
appserver.eam.url=appserverdcs://URL returned in step 4/as-eam
```

6 Run `yab update`.

Note If the configuration has not been set up correctly, the AppServers will not come online and the update will fail.

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 183.
- Specify user IDs or roles in Site Security Maintenance (36.3.13.8). See page 186.
- Specify user IDs or roles in GL Account Security Maintenance (36.3.13.1). See page 197.
- Specify user IDs or roles in Inventory Movement Code Security (36.3.13.13). See page 198.

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 18.

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 8.1
Sample Uses of User ID and Role Name

String	Description
`*`	All users have access.
`mary, manager`	Only user mary and members of the manager role have access.
`!jcd,*`	Everyone but user jcd has access.

The inverse of the last example does not work. If you put `*,!jcd` in the field, the system grants everyone access first and does not go back to check on `jcd`. Someone using the `jcd` user ID would not be excluded. In general, avoid using any exclamation point after the very beginning of the entry.

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 151 for details on securing fields in Adaptive UX.

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.

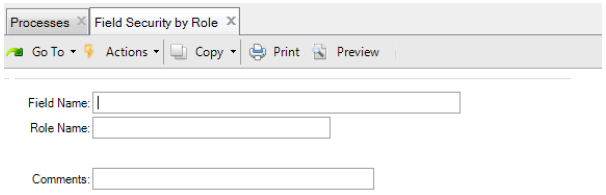
Field Security by Role

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. 8.1
Field Security by Role (36.3.15.2)



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).

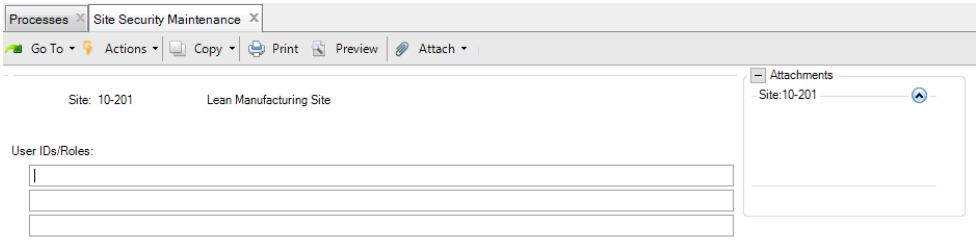
Access by Site

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. 8.2
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 186.

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 189 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 190 for details.
- Inventory details. See “Inventory Detail Restriction Maintenance” on page 191 for details.
- Issues and receipts. See “Unplanned Issue/Receipt Restriction Maintenance” on page 192 for details.
- Maintaining all types of purchase orders. See “PO Restriction Maintenance” on page 193 for details.
- Receipt handling and status change. See “PO Receipts Restriction Maintenance” on page 193 for details.
- Maintaining sales order, invoice, and quote lines. See “SO Restriction Maintenance” on page 194 for details.
- Creating shipments and maintaining shippers. See “SO Shipments Restriction Maintenance” on page 195 for details.
- Maintaining distribution orders (DO). See “DO Restriction Maintenance” on page 195 for details.
- Creating DO shipments. See “DO Shipments Restriction Maintenance” on page 195 for details.
- Creating DO receipts. See “DO Receipts Restriction Maintenance” on page 196 for details.
- Maintaining records, creating receipts, and completing shipments in SSM. See “SSM Restriction Maintenance” on page 196 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.

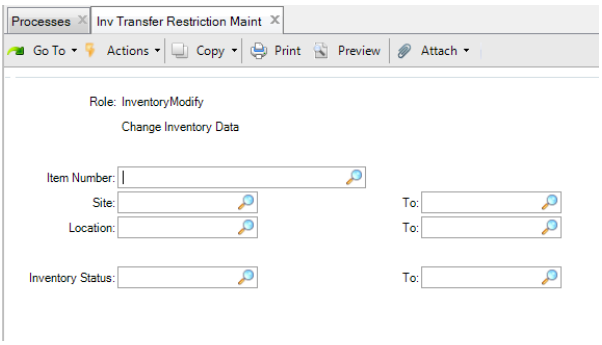
Inventory Transfer Restriction Maintenance

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. 8.3
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

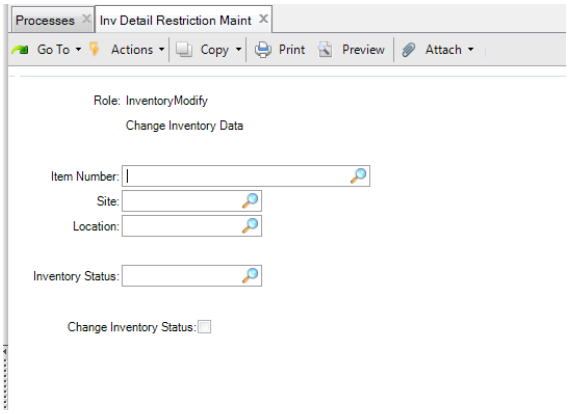
Use Inventory Detail Restriction Maintenance (36.3.7.2) to specify role-based restrictions on updating inventory details in these programs:

- 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 checkbox 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. 8.4
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 checkbox displays the list of target status codes that are allowed and lets you add or remove codes as required.

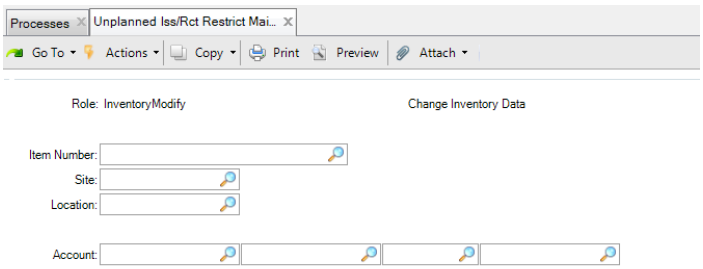
Status Code. Enter a status code to add to the list of valid target status codes that the current code can be changed to. The list is part of an update restriction defined for a particular role and combination of item, site, and location.

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. 8.5
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.

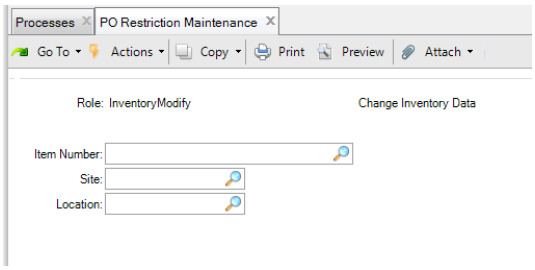
The account number is used when applying update restrictions to programs such as Issues–Unplanned (3.7) and Receipts–Unplanned (3.9). Define projects in Project Create (25.3.11.1.1).

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. 8.6
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:

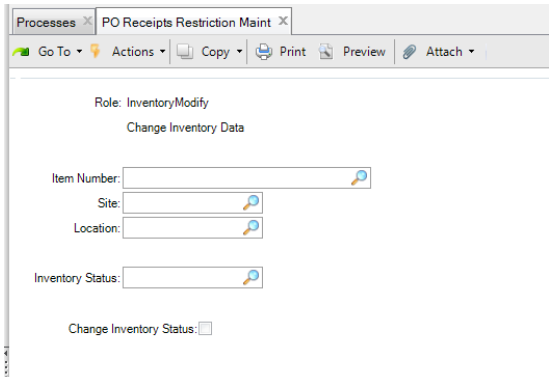
- Purchase Order Receipts (5.13.1)

- 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 checkbox 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 checkbox is not selected, the system deletes the list of valid To status codes defined for the current role, item, and value combination.

Fig. 8.7
PO Receipts Restriction Maintenance (36.3.7.6)

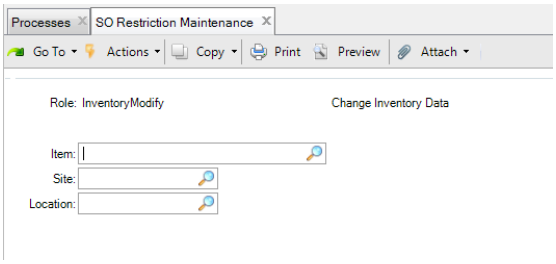


SO Restriction Maintenance

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. 8.8
SO Restriction Maintenance (36.3.7.8)

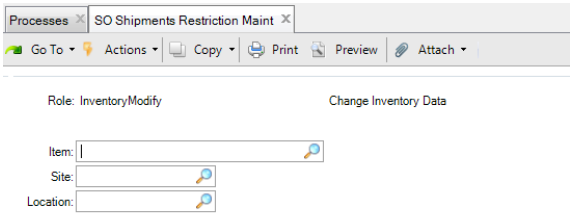


SO Shipments Restriction Maintenance

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. 8.9
SO Shipments Restriction Maintenance (36.3.7.9)

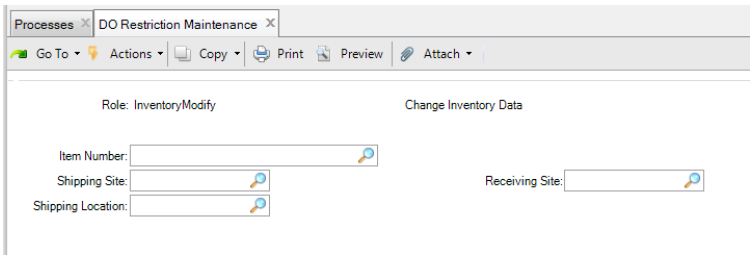


DO Restriction Maintenance

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. 8.10
DO Restriction Maintenance (36.3.7.13)

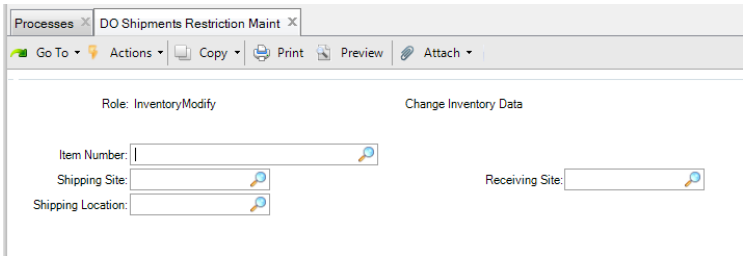


DO Shipments Restriction Maintenance

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. 8.11
DO Shipments Restriction Maintenance (36.3.7.14)

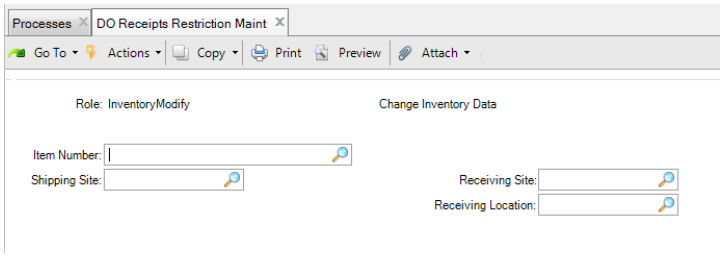


DO Receipts Restriction Maintenance

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. 8.12
DO Receipts Restriction Maintenance (36.3.7.15)

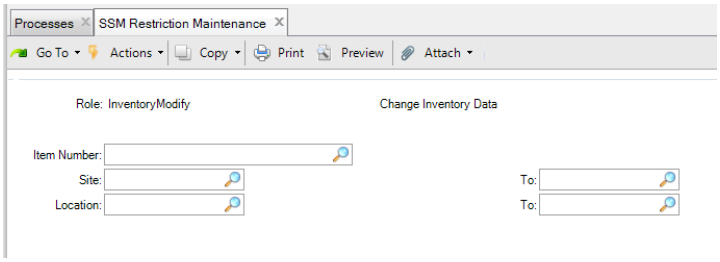


SSM Restriction Maintenance

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. 8.13
SSM Restriction Maintenance (36.3.7.17)

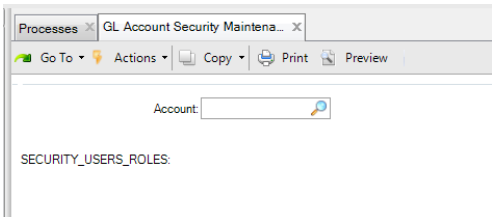


Defining GL Account Security

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. 8.14
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.

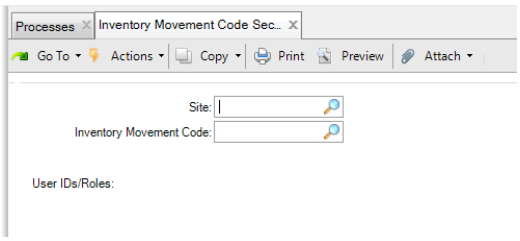
If no account security has been defined, all users and roles are permitted to update the account, within the parameters of other restrictions.

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. 8.15
Inventory Movement Code Security (36.3.13.13)



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.

Chapter 9

Segregation of Duties in Adaptive ERP

This section describes how to configure and set up segregation of duties in Adaptive ERP. Segregation of duties is an internal control that prevents a single user from performing two or more phases of a transaction or operation.

Overview 201
Explains the purpose of segregation of duties, including usage examples. Introduces key segregation of duties concepts.

Plan a Segregation of Duties System 205
Outlines how to plan your segregation of duties system by creating a high-level overview of your business environment.

Segregation of Duties Rule Checking 206
Discusses the role permissions and role membership rules that segregation of duties enforces.

Complete Prerequisite Activity 212
Describes the prerequisites that must be met before you can implement segregation of duties.

Activate Segregation of Duties 212
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 214
Outlines how to create, modify, view, and delete segregation of duties categories.

Assign Resources to Segregation of Duties Categories 218
Describes how to associate an application resource with a segregation of duties category.

Maintain the Segregation of Duties Matrix 221
Discusses how to define the compatibility of segregation of duties categories.

Define Role Permissions 224
Outlines how the associations between roles and functions are constrained by segregation of duties policy.

Define Role Membership 225
Describes how the associations between users and roles are constrained by segregation of duties policy.

Maintain Segregation of Duties Policy Exceptions 225
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 227
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 228
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 235
Lists the reports and views that let you review segregation of duties violations.

Archive Log Record Files 239
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 strong internal controls into their business processes. Among these internal controls is segregation of duties.

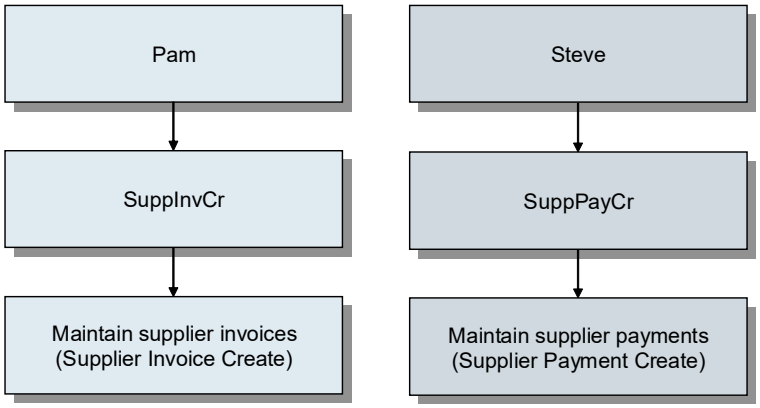
Segregation of duties refers to the notion that the duties of individuals in an organization should be limited to certain areas of responsibility, so as to minimize the ability of any individual to misappropriate company property. Segregation of duties prevents a single user from performing two or more phases of a transaction or operation. See “Segregation of Duties Verification” on page 202 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 9.1 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.

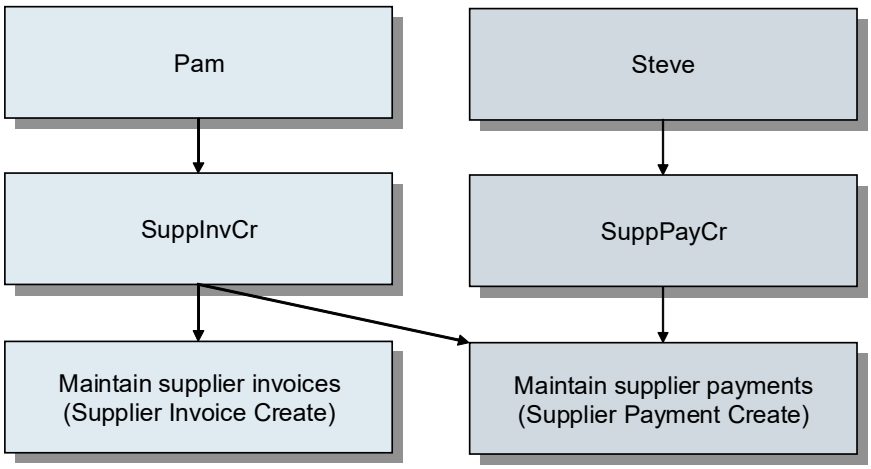
Fig. 9.1
Segregation of Duties Example



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 9.2 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. 9.2
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 Block SOD 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 206 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 221.

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.

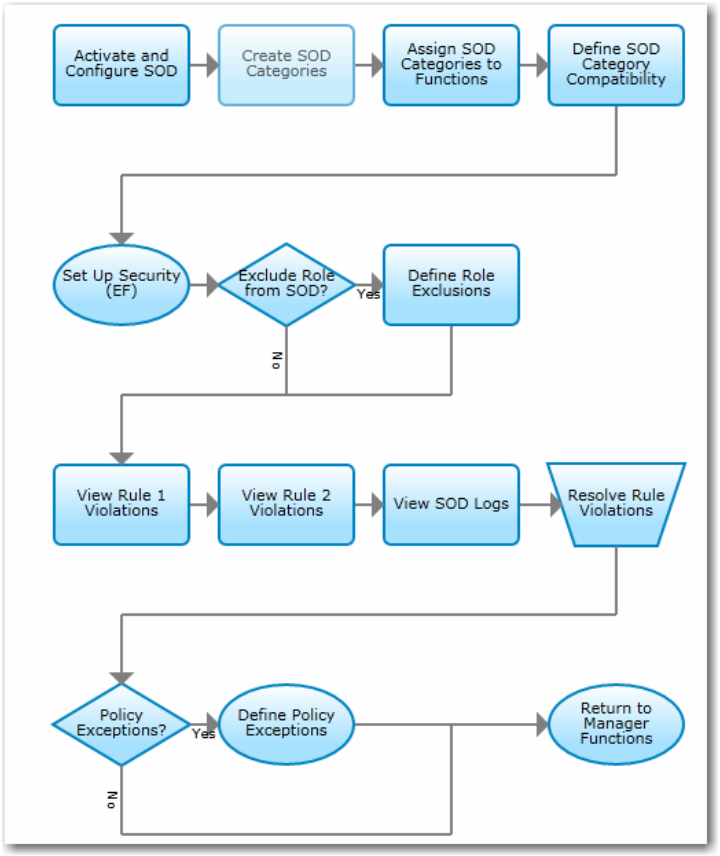
See “Maintain Segregation of Duties Policy Exceptions” on page 225.

Segregation of Duties Process Workflow

Important If your QAD Adaptive ERP system includes Adaptive UX, perform all segregation of duties setup in Adaptive UX. When you import the SOD Matrix of incompatible categories into Adaptive UX, Adaptive UX searches for conflicts across both Adaptive UX and Enterprise Edition resources. Currently, if you import the matrix through Adaptive ERP, only conflicts with Enterprise Edition resources are identified. See Chapter 10, “Segregation of Duties in Adaptive UX,” on page 241 for detailed instructions.

Use the options in the Segregation of Duties menus in QAD Adaptive ERP to set up segregation of duties and to configure segregation of duties functions. Figure 9.3 illustrates one possible segregation of duties process workflow; use it to set up segregation of duties functions in your environment.

Fig. 9.3
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 205. For details on planning and implementing security in your system, see “Implementation Summary” on page 6.

After you create user records 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 from QAD Adaptive ERP” on page 212.

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 214.

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 224.

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 221.

The next step is to define role permissions in your system. This associates application resources to user roles. See “Define Role Permissions” on page 101. 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 227.

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 225.

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. See “Report and View Logs and Violations” on page 235.

Segregation of duties violations that arise during segregation of duties maintenance are recorded in a log. Use SOD Log Archive (36.3.27.7) action to archive log table records. See “Archive Log Record Files” on page 239.

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 Services delivers a set of default roles and segregation of duties categories that facilitate the implementation of segregation of duties. You can load the provided segregation of duties data using SOD Import/Export (36.3.27.15). If your QAD Adaptive ERP instance is not integrated with Adaptive UX, see “Import and Export Segregation of Duties Data” on page 228. If your environment includes Adaptive UX, see “SOD Setup” on page 264 for segregation of duties setup in Adaptive UX.

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

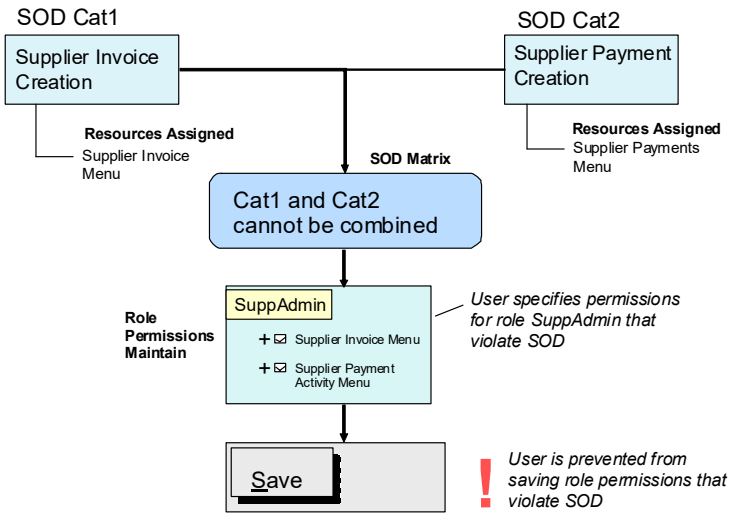
When you add a resource to the list of resources allowed for a role in Role Permissions Maintain (36.3.6.5), the system validates the assignment to verify that all the role resources belong to compatible segregation of duties categories (Rule 1 validation). If Rule 1 is violated, the system blocks the 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 Block SOD Violations checkbox 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. 9.4
Role Permissions Validation



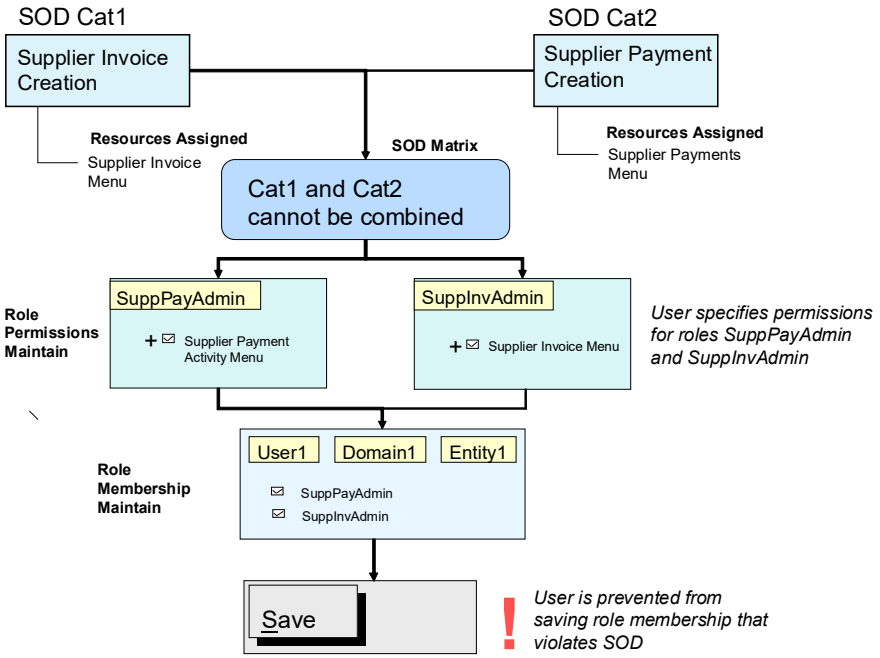
Role Membership Validation

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 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 Block SOD Violations checkbox is selected in SOD Configuration (36.3.27.14), you are blocked from performing steps that violate role membership compatibility.

Fig. 9.5
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 Block SOD Violations checkbox in SOD Configuration (36.3.27.14).

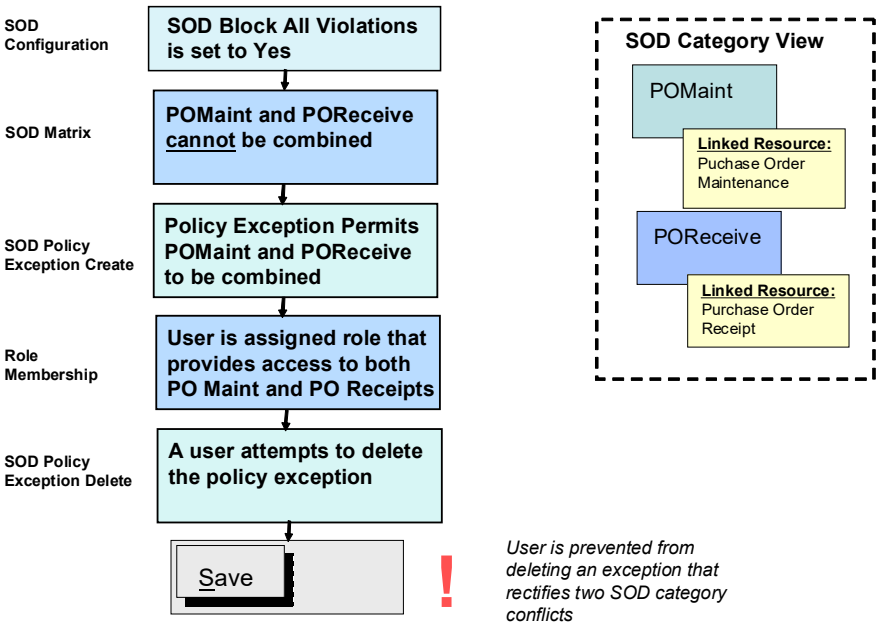
Indirect violations occur if you perform actions that violate segregation of duties rules using screens other than Role Permissions Maintain (36.3.6.5) and Role Membership Maintain. However, role membership (Rule 2) violations caused by updates in Role Permissions Maintain (36.3.6.5) are also examples of indirect violations.

Figure 9.6 shows how the system handles an indirect violation when the Block SOD 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. 9.6
Indirect Segregation of Duties Violation



Segregation of Duties Rule Matrix

Table 9.1 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 9.1
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 clear 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

Ensure OpenEdge is using TLSv1.2. TLSv1.3 is not supported for segregation of duties. Enter the following settings in the `configuration.properties` file and then run `yab update`.

```
openedge.env.pscsslclient.key=PSC_SSLCLIENT_PROTOCOLS
openedge.env.pscsslclient.value=TLSv1.2
```

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 104.

You also can define user roles—but not role permissions or role membership—as a prerequisite activity. See “Define Roles” on page 93.

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 227.

Important If you attempt to activate segregation of duties and the Excluded from SOD field is not selected for the SuperUser role, a warning displays to indicate that the activation may not process correctly.

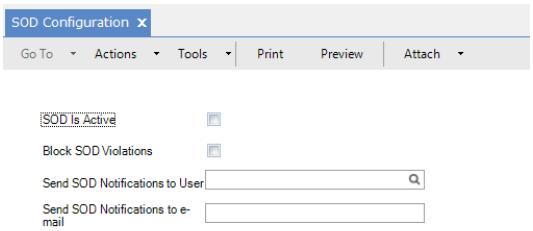
Activate Segregation of Duties

Segregation of Duties can be activated from Adaptive UX, Adaptive ERP, and the command line. If your QAD Adaptive ERP system includes Adaptive UX, do all segregation of duties setup in Adaptive UX. When you import the SOD Matrix of incompatible categories into Adaptive UX, Adaptive UX searches for conflicts across both Adaptive UX and Enterprise Edition resources. Currently, if you import the matrix through Adaptive ERP, only conflicts with Enterprise Edition resources are identified.

Activate Segregation of Duties from QAD Adaptive ERP

Use SOD Configuration (36.3.27.14) to activate segregation of duties rule checking on your system.

Fig. 9.7
SOD Configuration (36.3.27.14)



SOD Is Active. Select the checkbox 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.

Block SOD Violations. Select this checkbox 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 Block SOD 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 Block SOD Violations field cannot be enabled until these violations are fixed.

If you leave the field clear, 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 clear.

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 emails 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 emails to an external email address, specify the email 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
PROTERMCAP=<PROGRESS_LOCATION>/protermcap;export PROTERMCAP

<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

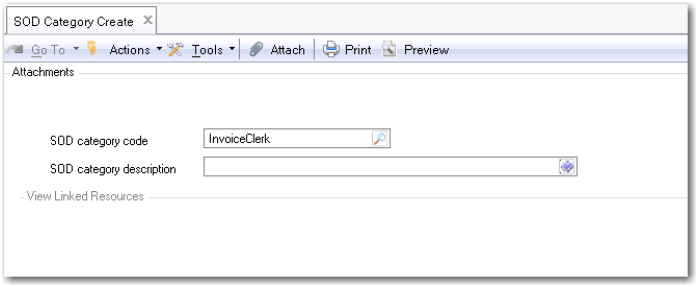
Segregation of duties category maintenance involves creating, modifying, viewing and deleting categories.

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. 9.8
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. 9.9
SOD Category View, View Linked Resources Drop-Down

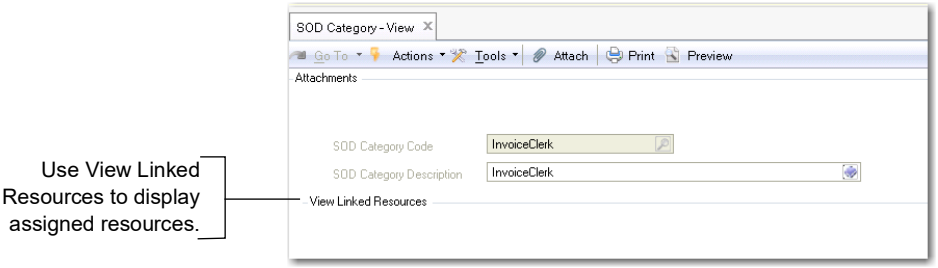
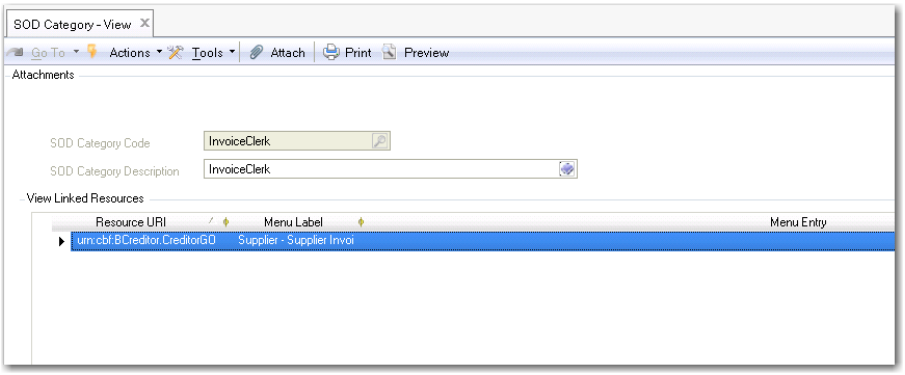


Fig. 9.10
SOD Category View, Linked Resources



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 to delete a category that is associated with a resource, a message displays and you cannot proceed.

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.

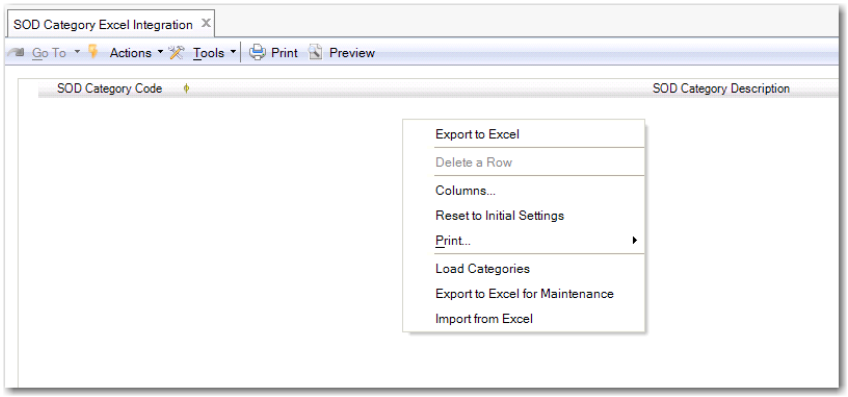
In QAD Adaptive ERP, you can right-click and select Load Categories, to see all segregation of duties categories in the grid. You can then modify and save the segregation of duties category records.

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 name headings for maintaining data.

In Adaptive ERP, you can right-click and select Import from Excel, and then 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. 9.11
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). Then specify the category incompatibilities 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.

Assigning Resources in QAD Adaptive ERP

In QAD Adaptive ERP, an application resource can be associated with one category or with no category.

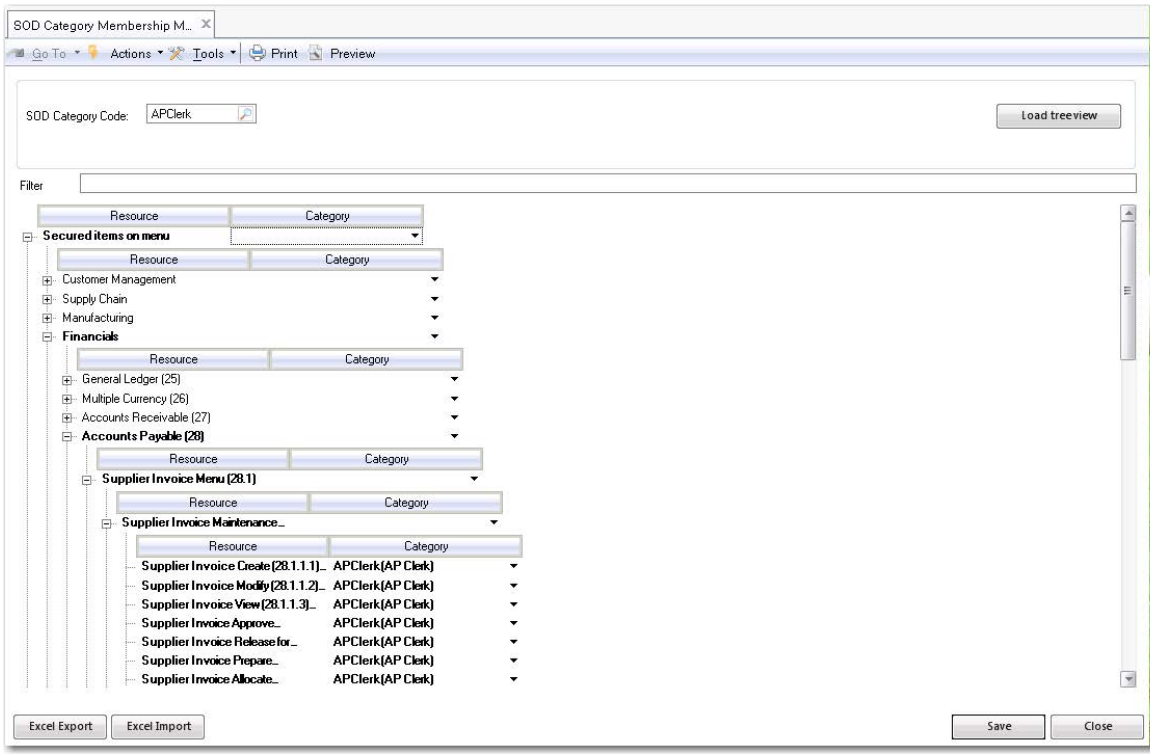
- If associated with a category, the resource is only compatible with other resources that are associated with resources with the same segregation of duties category, with resources that have a compatible segregation of duties category, and with all resources that are not linked to a segregation of duties 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.

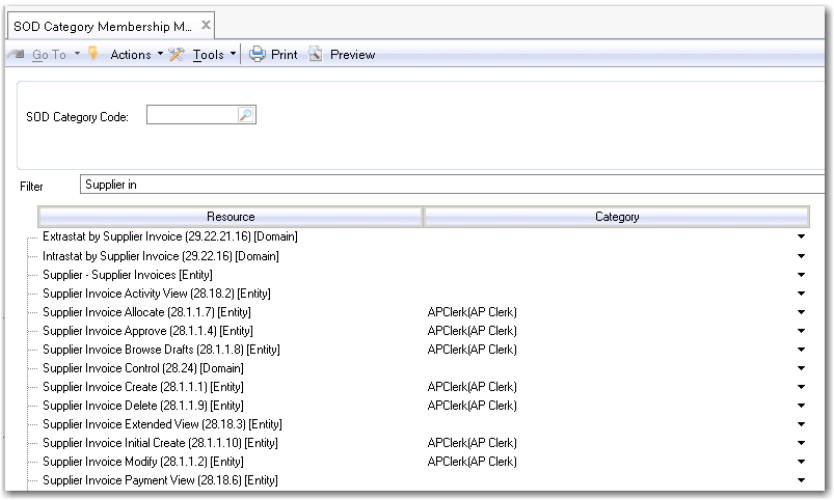
To assign a category to a menu resource, select the category from the drop-down list to the right of the resource name.

Fig. 9.12
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. 9.13
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

Excel integration allows you to export resource and segregation of duties category data to Excel, maintain the data offline, and re-import the data.

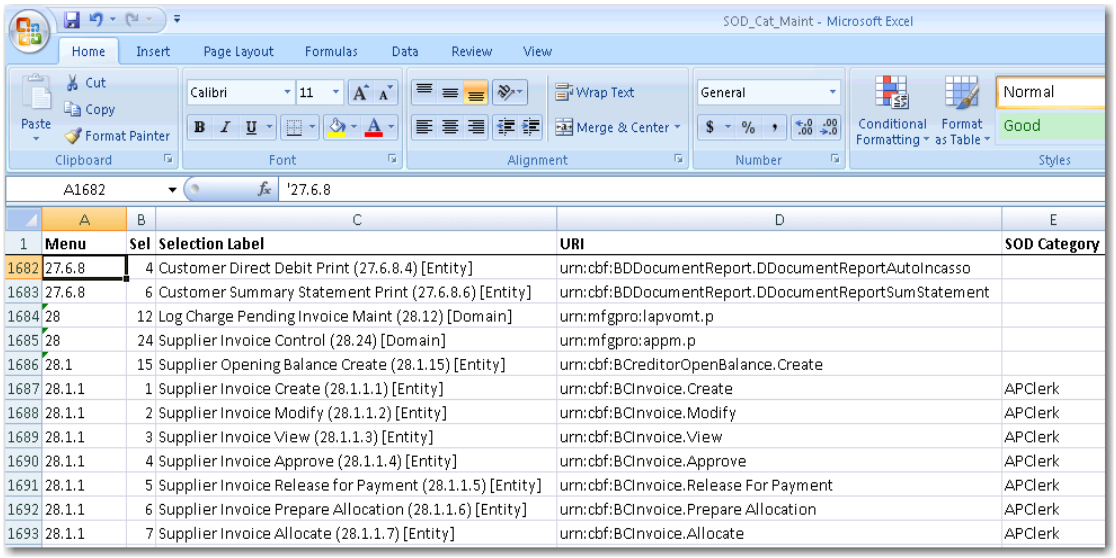
SOD Category Membership Maintain (36.3.27.4) contains options that let you export resource and segregation of duties category data to Excel, maintain the data offline, and re-import the data using Excel integration.

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. 9.14
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:lapvomt.p	
1685	28	24	Supplier Invoice Control (28.24) [Domain]	urn:mfgpro:appm.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.

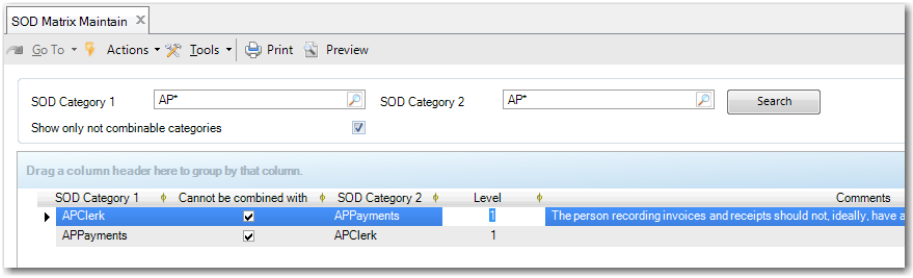
If you click the Search button in the header, all the segregation of duties category pairs currently defined in the system and their corresponding compatibilities are displayed.

You can then use the checkbox 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 “.”.

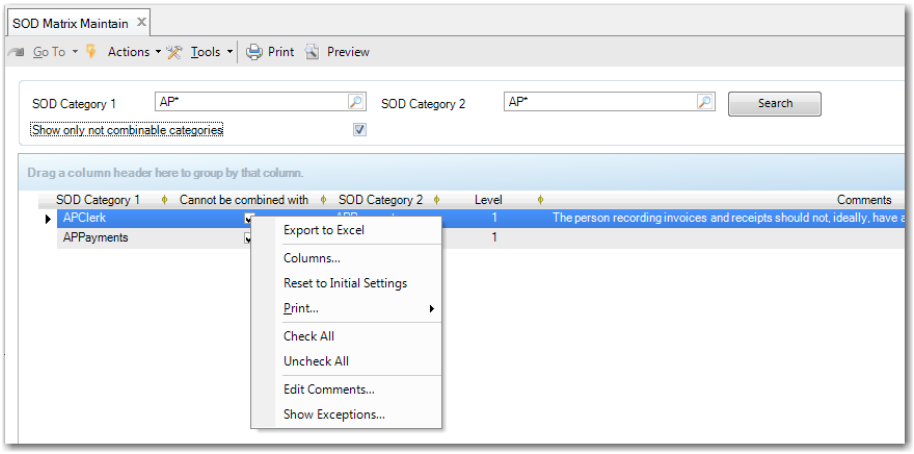
If you search on all categories or search using wildcards for two similarly-named categories, a segregation of duties category combination can appear twice in the grid; for example, one entry for InvoiceEntry-InvoiceAppr and another entry for InvoiceAppr-InvoiceEntry, based on the example in Figure 9.15. 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. 9.15
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. 9.16
SOD Matrix Maintain, Context Menu



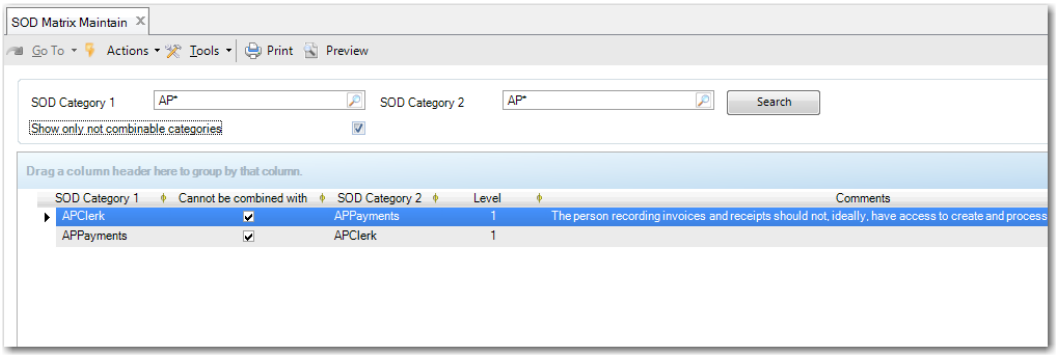
When you save new information, the system checks to see if segregation of duties policy violations have been introduced based on existing category assignments to application resources, resource assignments to roles, and user assignments to roles.

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 Block SOD 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. 9.17
SOD Matrix Maintain (36.3.27.3)



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.

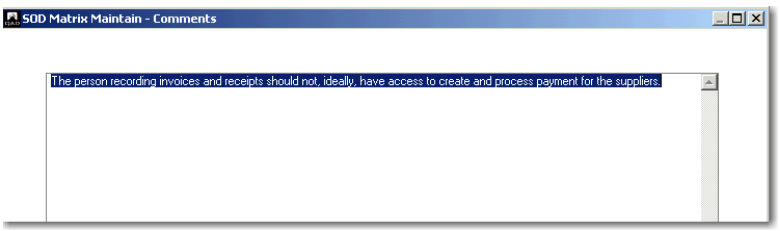
Level. Enter a value from 1 to 5 to associate a conflict level with the mutually exclusive category codes.

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 clear 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. 9.18
SOD Matrix Maintain, Comments Dialog

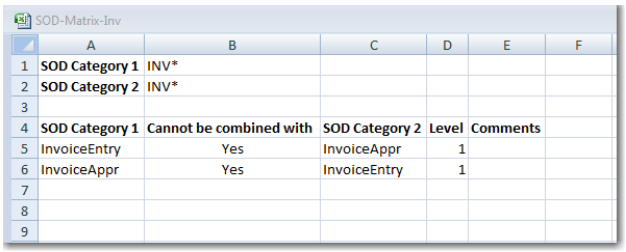


SOD Matrix Excel Integration

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. 9.19
SOD Matrix Maintain Excel Spreadsheet



SOD-Matrix-Inv

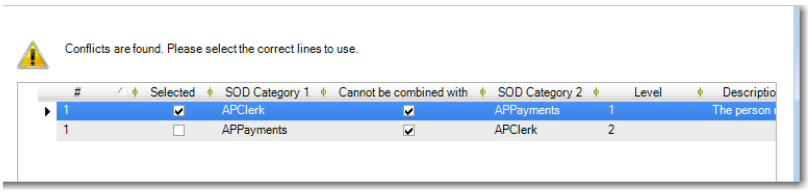
	A	B	C	D	E	F
1	**SOD Category 1**	INV*				
2	**SOD Category 2**	INV*				
3						
4	**SOD Category 1**	**Cannot be combined with**	**SOD Category 2**	**Level**	**Comments**	
5	InvoiceEntry	Yes	InvoiceAppr	1		
6	InvoiceAppr	Yes	InvoiceEntry	1		
7						
8						
9						

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. 9.20
SOD Matrix Maintain, Conflicts



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 9.20, 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 101 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 221 for QAD Adaptive ERP.

If a user has been assigned one or more roles, the user can be assigned to the role only if each of the 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 119.

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.

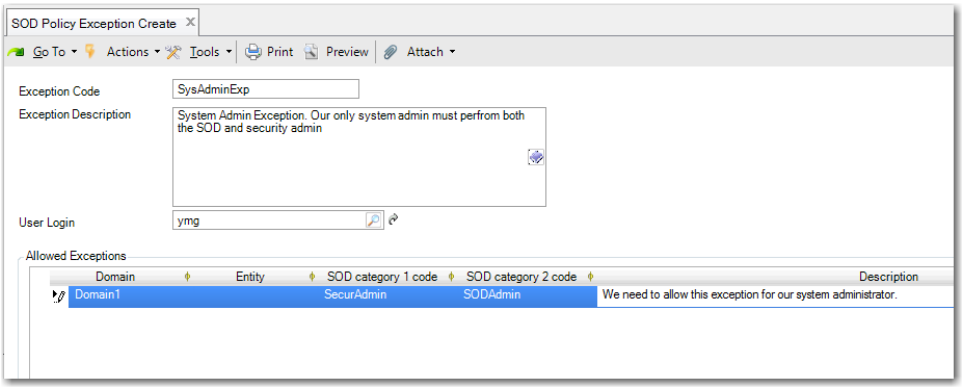
Policies are checked any time a change is made that impacts segregation of duties; for example, when a user is assigned to a role, when you link resources to categories, when you change role permissions, or when you change role membership.

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.

SOD Policy Exceptions

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. 9.21
SOD Policy Exception Create (36.3.27.2.1)



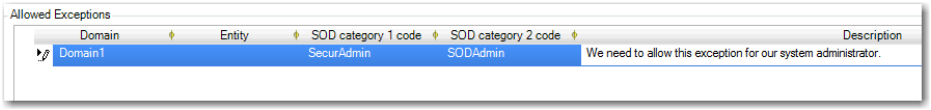
Exception Code. Enter a policy exception code.

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. 9.22
SOD Policy Exception Create, Category Details



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 119.

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.

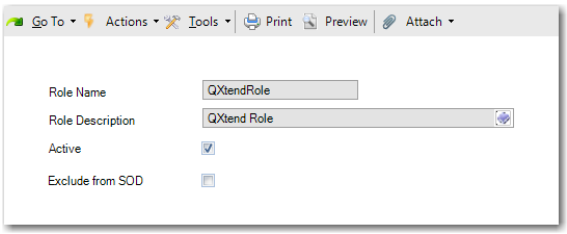
Segregation of Duties Role Exclusions

You can specify particular roles to be 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.

Use SOD Role Exclusion (36.3.27.8) to specify that a particular role is exempt from segregation of duties rule checks and blocking.

Segregation of duties role exclusion is the highest level of segregation of duties policy exception and should be used carefully.

Fig. 9.23
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 Block SOD Violations checkbox is selected in SOD Configuration (36.3.27.14).

If the Block SOD Violations checkbox 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) in QAD Adaptive ERP 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.

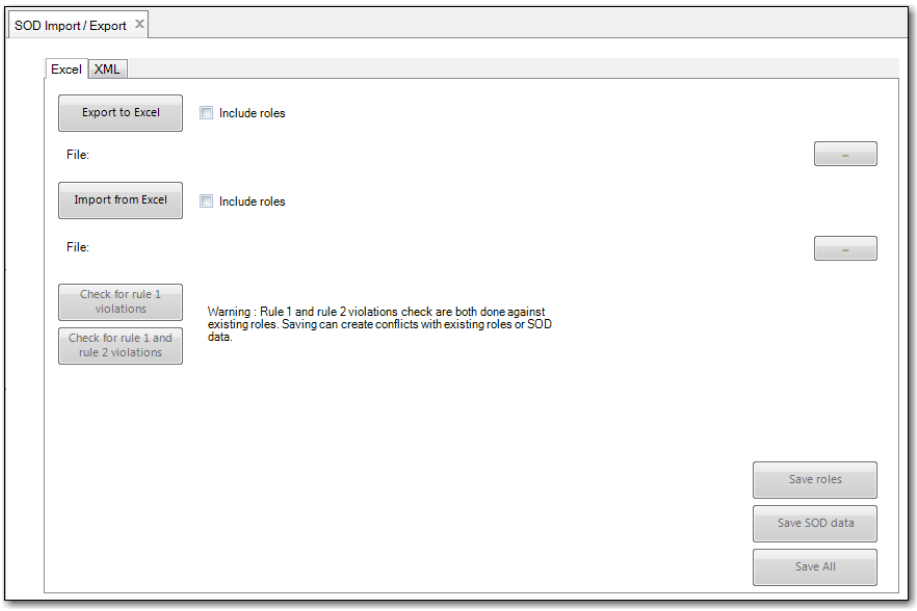
You can export segregation of duties data to an XML file to create default XML data that can be loaded during the deployment process. You also can import data from an XML file, which facilitates the loading of default SOD data. If you reload the default SOD data after you have modified SOD categories 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

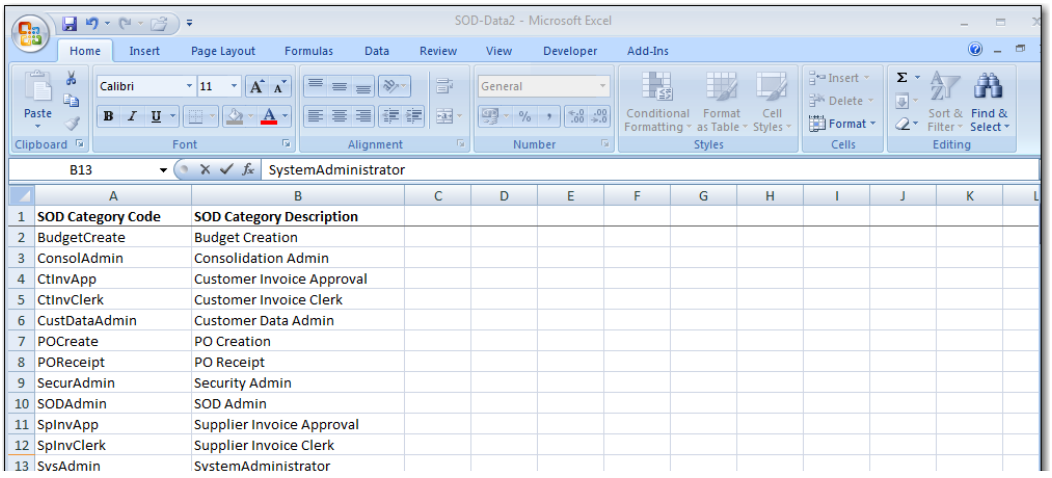
Fig. 9.24
SOD Import/Export (36.3.27.15)



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. 9.25
SOD Category Worksheet

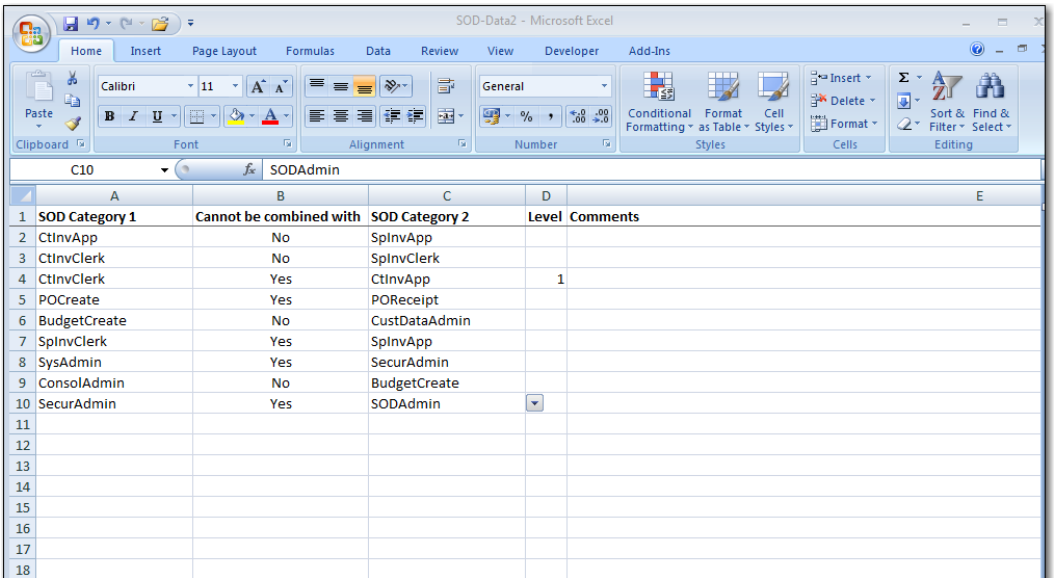


	A	B
1	**SOD Category Code**	**SOD Category Description**
2	BudgetCreate	Budget Creation
3	ConsolAdmin	Consolidation Admin
4	CtInvApp	Customer Invoice Approval
5	CtInvClerk	Customer Invoice Clerk
6	CustDataAdmin	Customer Data Admin
7	POCreate	PO Creation
8	POReceipt	PO Receipt
9	SecurAdmin	Security Admin
10	SODAdmin	SOD Admin
11	SpInvApp	Supplier Invoice Approval
12	SpInvClerk	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 223 for more information on SOD Matrix Excel integration.

Fig. 9.26
SOD Matrix Worksheet



SOD-Data2 - Microsoft Excel

Home | Insert | Page Layout | Formulas | Data | Review | View | Developer | Add-Ins

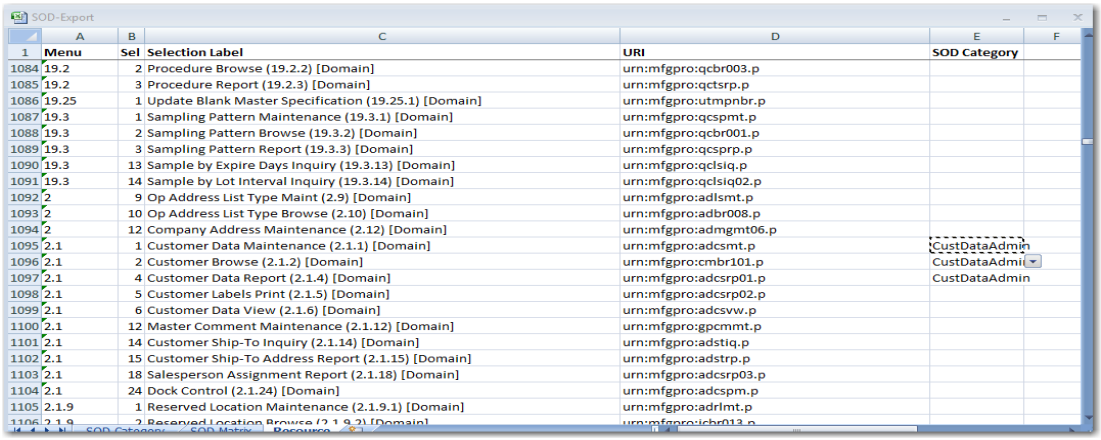
C10 | SODAdmin

	A	B	C	D	E
1	SOD Category 1	Cannot be combined with	SOD Category 2	Level	Comments
2	CtInvApp	No	SpInvApp		
3	CtInvClerk	No	SpInvClerk		
4	CtInvClerk	Yes	CtInvApp	1	
5	POCreate	Yes	POReceipt		
6	BudgetCreate	No	CustDataAdmin		
7	SpInvClerk	Yes	SpInvApp		
8	SysAdmin	Yes	SecurAdmin		
9	ConsolAdmin	No	BudgetCreate		
10	SecurAdmin	Yes	SODAdmin		
11					
12					
13					
14					
15					
16					
17					
18					

Resource Worksheet

In the Resource spreadsheet, you can only add or remove segregation of duties categories. See “SOD Category Membership Excel Integration” on page 220.

Fig. 9.27
Resource Worksheet



SOD-Export

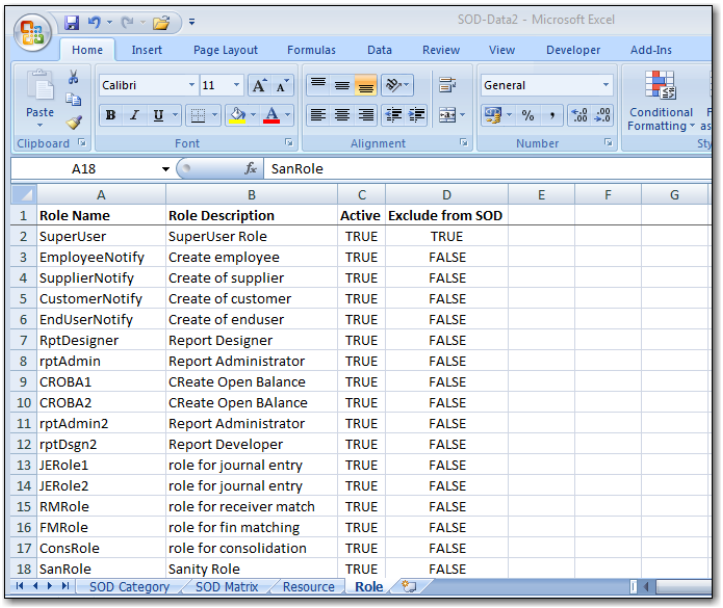
	A	B	C	D	E	F
1	Menu	Sel	Selection Label	URI	SOD Category	
1084	19.2	2	Procedure Browse (19.2.2) [Domain]	urn:mfgpro:qcbr003.p		
1085	19.2	3	Procedure Report (19.2.3) [Domain]	urn:mfgpro:qctsrp.p		
1086	19.25	1	Update Blank Master Specification (19.25.1) [Domain]	urn:mfgpro:utmpnbr.p		
1087	19.3	1	Sampling Pattern Maintenance (19.3.1) [Domain]	urn:mfgpro:qcspmt.p		
1088	19.3	2	Sampling Pattern Browse (19.3.2) [Domain]	urn:mfgpro:qcbr001.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	CustDataAdmin	
1096	2.1	2	Customer Browse (2.1.2) [Domain]	urn:mfgpro:cmbr101.p	CustDataAdmi	
1097	2.1	4	Customer Data Report (2.1.4) [Domain]	urn:mfgpro:adcsrp01.p	CustDataAdmin	
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:adstrp.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:adcspm.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:icbr013.p		

SOD_Category | SOD_Matrix | Resource

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 227.

Fig. 9.28
Role Worksheet



SOD-Data2 - Microsoft Excel

Home | Insert | Page Layout | Formulas | Data | Review | View | Developer | Add-Ins

A18: SanRole

	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	CReate Open Balance	TRUE	FALSE			
10	CROBA2	CReate 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			

SOD Category | SOD Matrix | Resource | Role

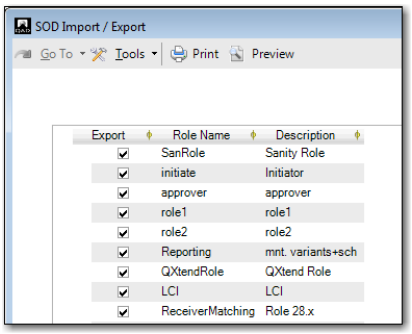
Export to Excel

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 checkbox, the system displays a dialog that lets you specify the roles for which to export data.

Fig. 9.29
SOD Import/Export, Role Selection



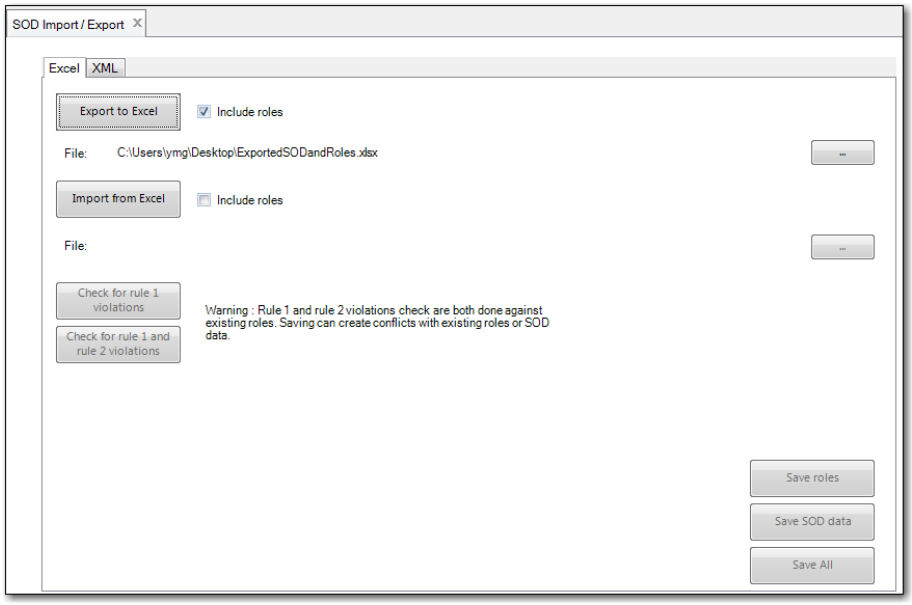
SOD Import / Export

Go To | Tools | Print | Preview

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. 9.30
Name and Path of Exported Excel File



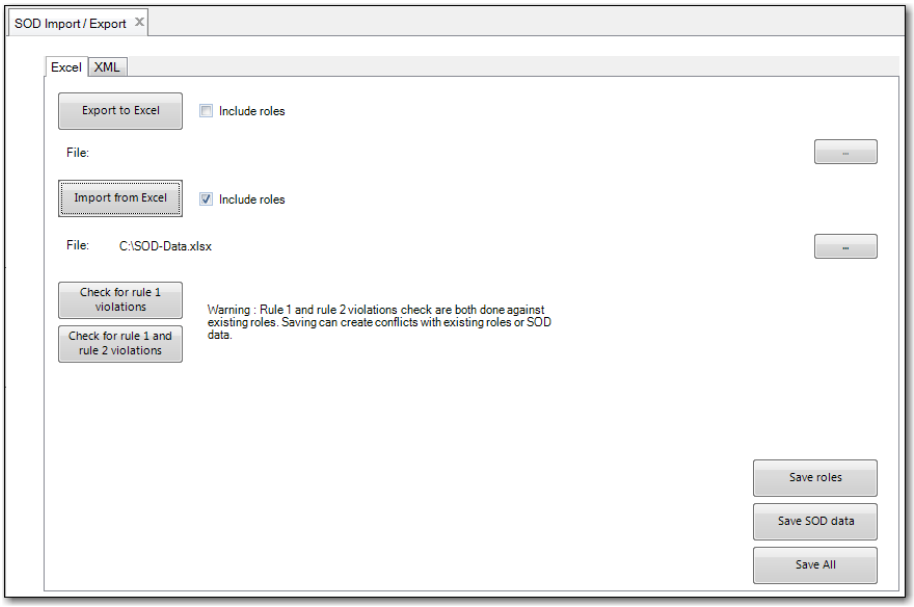
Import from Excel

Use the Import from Excel option to load an Excel spreadsheet of segregation of duties default data.

If you select the Include Roles checkbox, 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.

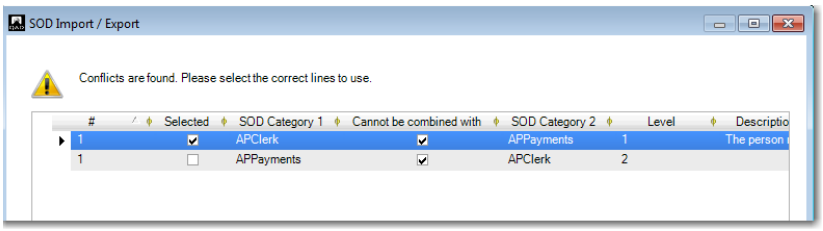
When you load a spreadsheet, the Check for Violations buttons are activated. Click the buttons to determine if the loaded data generates segregation of duties violations.

Fig. 9.31
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 clear the compatibility indicator, but do not make an identical modification to the other row, the system displays a screen indicating that conflicts exist.

Fig. 9.32
SOD Import/Export, Conflicts



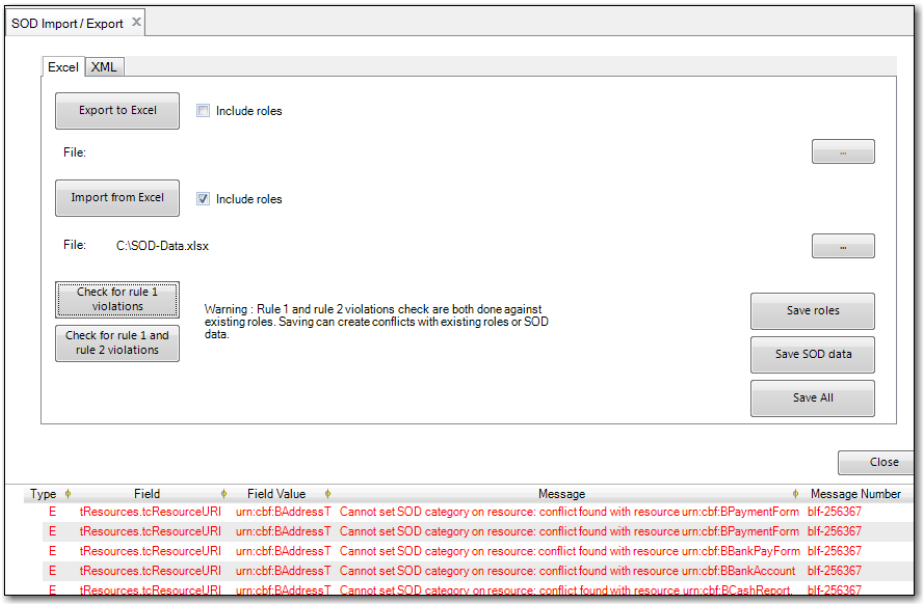
For every conflict found, you must indicate which of the conflicting pairs you want to import by selecting the Selected field.

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. 9.33
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. 9.34
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:

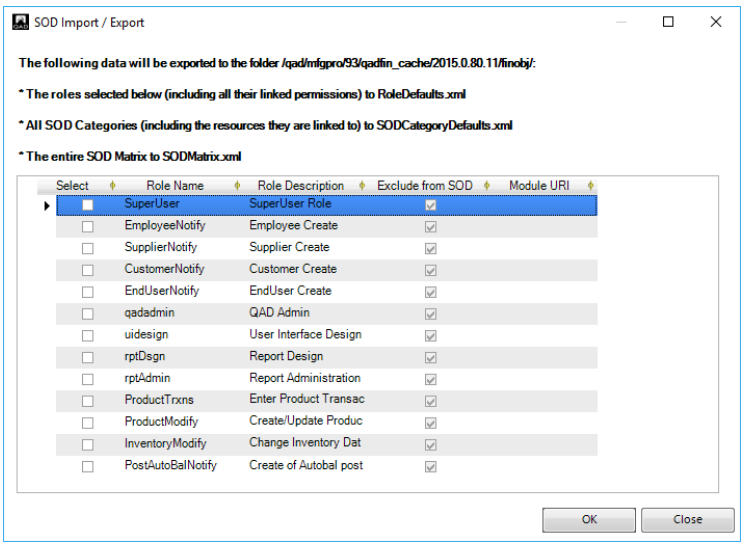
- Roles
- Role permissions
- Segregation of duties categories
- Segregation of duties matrix
- Segregation of duties resource linking

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. 9.35
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

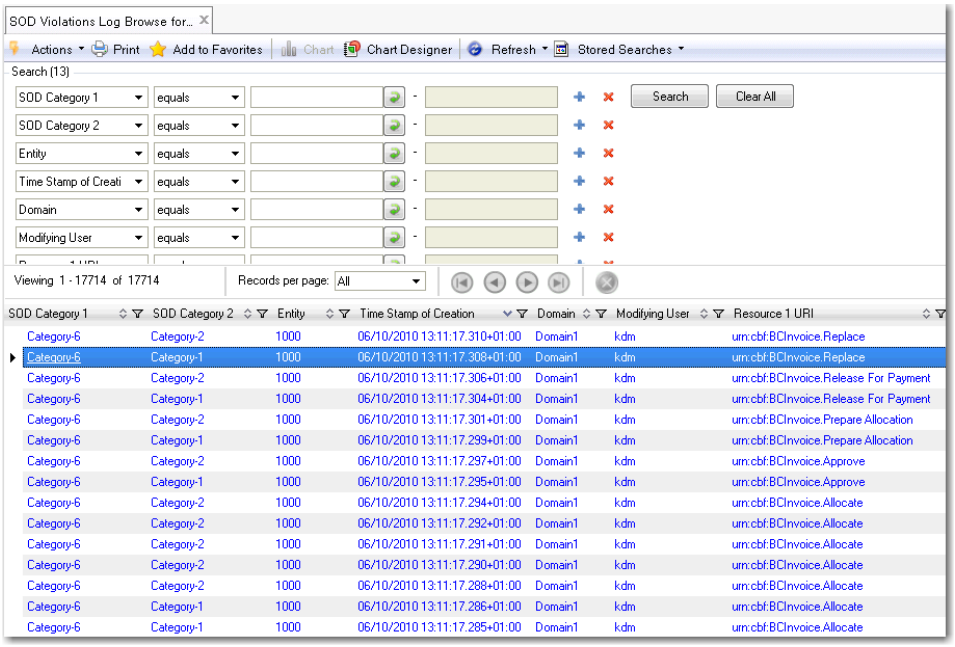
The SOD Log Viewer (36.3.27.6) lets you view logs of changes that impacted the segregation of duties rules over time, such as rule violations and actions that rectified rule violations.

The browse grid includes:

- 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. 9.36
SOD Log Viewer (36.3.27.6)



Report on Current Segregation of Duties Conflicts

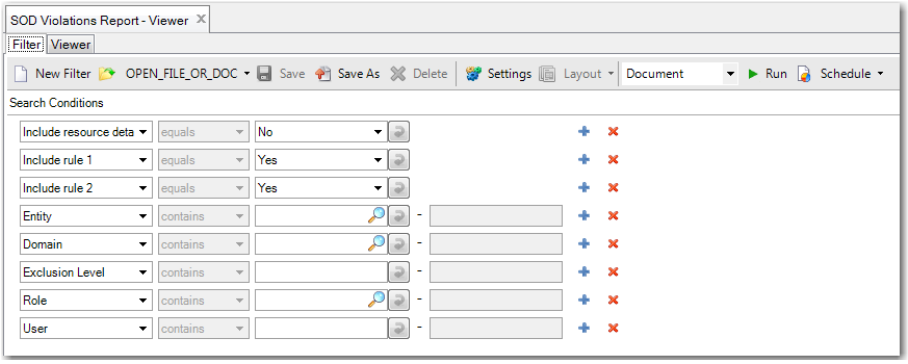
Use the SOD Violations report (36.3.27.9) to determine whether there are compliance violations for role permissions, role membership, or both in the system.

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 9.37 illustrates the selection criteria for the SOD Violations report (36.3.27.9).

Fig. 9.37
SOD Violation Report, Selection Criteria



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

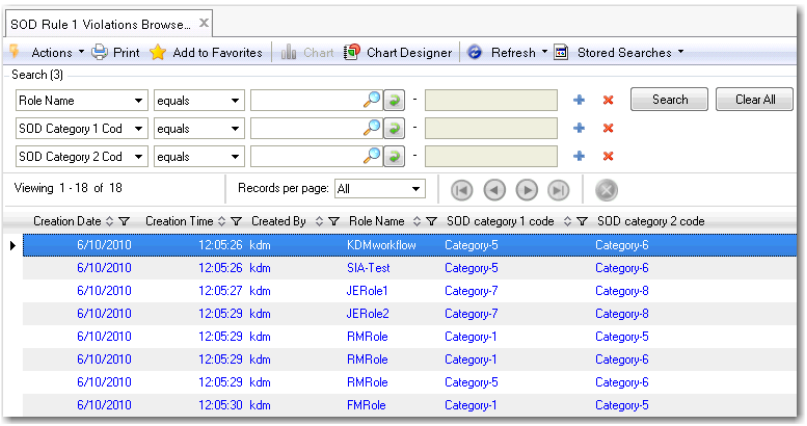
Category codes are displayed with their description. Resources are displayed with their corresponding menu entry and label.

Fig. 9.38
SOD Violations Report (36.3.27.9)

View Role Permissions Violations

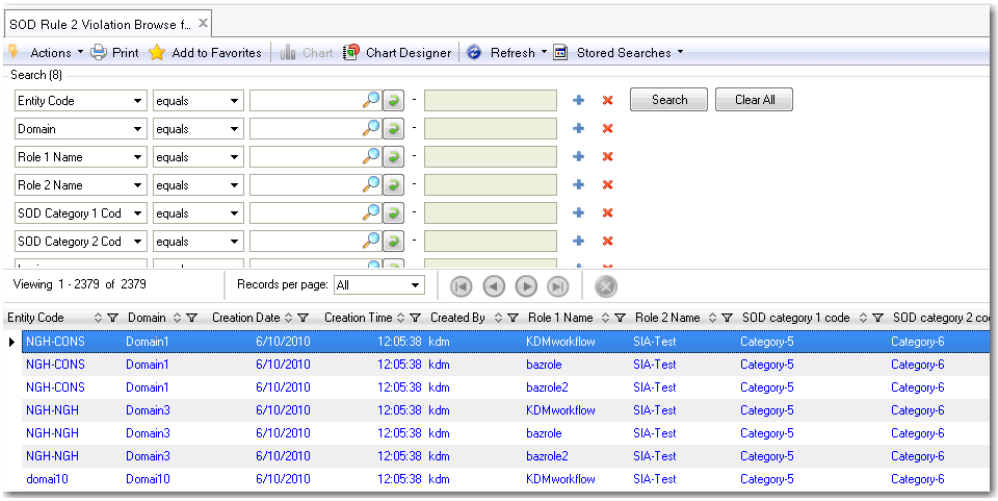
Use SOD Violations Rule 1 View (36.3.27.10) to display details of role permission violations.

Fig. 9.39
SOD Violations Rule 1 View (36.3.27.10)



Use SOD Violations Rule 2 View (36.3.27.11) to display details of role membership violations.

Fig. 9.40
SOD Violations Rule 2 View (36.3.27.11)



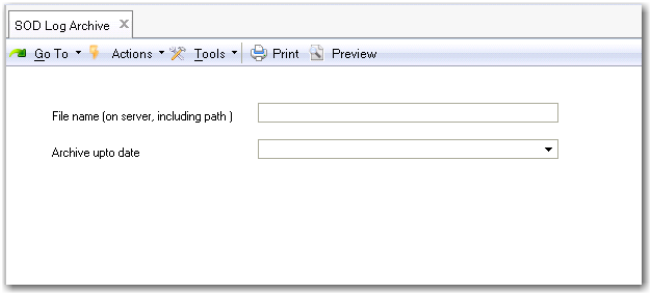
Archive Log Record Files

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. 9.41
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).

Chapter 10

Segregation of Duties in Adaptive UX

This chapter describes how to configure and set up segregation of duties in Adaptive UX. Segregation of duties is an internal control that prevents a single user from performing two or more phases of a transaction or operation.

Overview ***243***
Explains the purpose of segregation of duties, including usage examples. Introduces key segregation of duties concepts.

Plan a Segregation of Duties System ***247***
Outlines how to plan your segregation of duties system by creating a high-level overview of your business environment.

Segregation of Duties Rule Checking ***248***
Discusses the role permissions and role membership rules that segregation of duties enforces.

Complete Prerequisite Activity ***254***
Describes the prerequisites that must be met before you can implement segregation of duties.

Activate Segregation of Duties ***255***
Describes how to activate segregation of duties.

Maintain Segregation of Duties Categories ***256***
Outlines how to create, modify, view, and delete segregation of duties categories.

Assign Resources to Segregation of Duties Categories ***257***
Describes how to associate an application resource with a segregation of duties category.

Define Role Permissions ***260***
Outlines how the associations between roles and functions are constrained by segregation of duties policy.

Define Role Membership ***262***
Describes how the associations between users and roles are constrained by segregation of duties policy.

Maintain Segregation of Duties Policy Exceptions ***262***
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 264
Outlines how you can specify that a particular role is exempt from segregation of duties rule checks and blocking.

SOD Setup 264
Explains how to use Excel to download a spreadsheet template and upload segregation of duties data.

Import and Export Segregation of Duties Data 267
Describes how you can create and load default data for segregation of duties categories, matrices, roles, menus, and resource assignments using Excel.

Report and View Logs and Violations 272
Lists the reports and views that let you review segregation of duties violations.

Archive Log Record Files 275
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 strong internal controls into their business processes. Among these internal controls is segregation of duties.

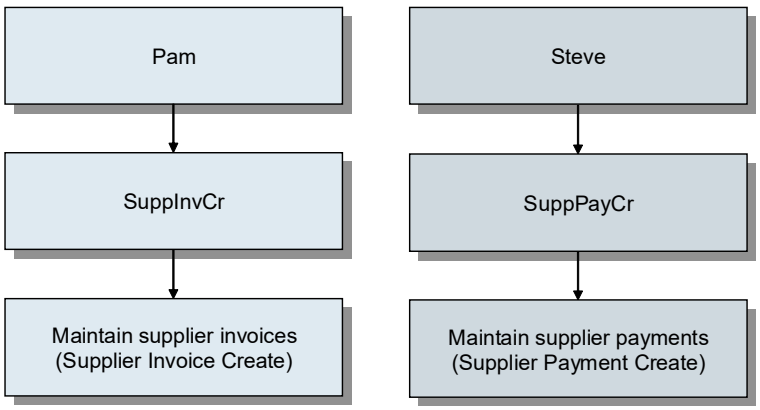
Segregation of duties refers to the notion that the duties of individuals in an organization should be limited to certain areas of responsibility, so as to minimize the ability of any individual to misappropriate company property. Segregation of duties prevents a single user from performing two or more phases of a transaction or operation. See “Segregation of Duties Verification” on page 244 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 10.1 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.

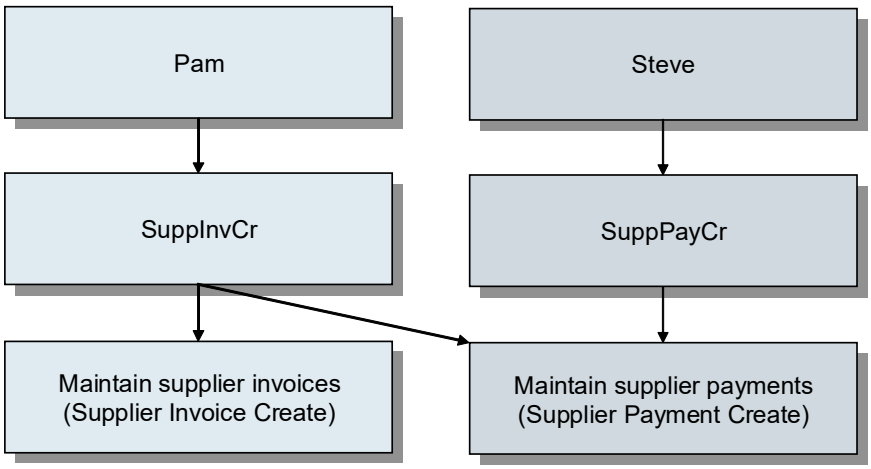
Fig. 10.1
Segregation of Duties Example



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 10.2 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. 10.2
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 Block Violations option on the SOD Control screen 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 248 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.

The segregation of duties category matrix is part of the SOD Setup screen. See “SOD Matrix” on page 266.

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.

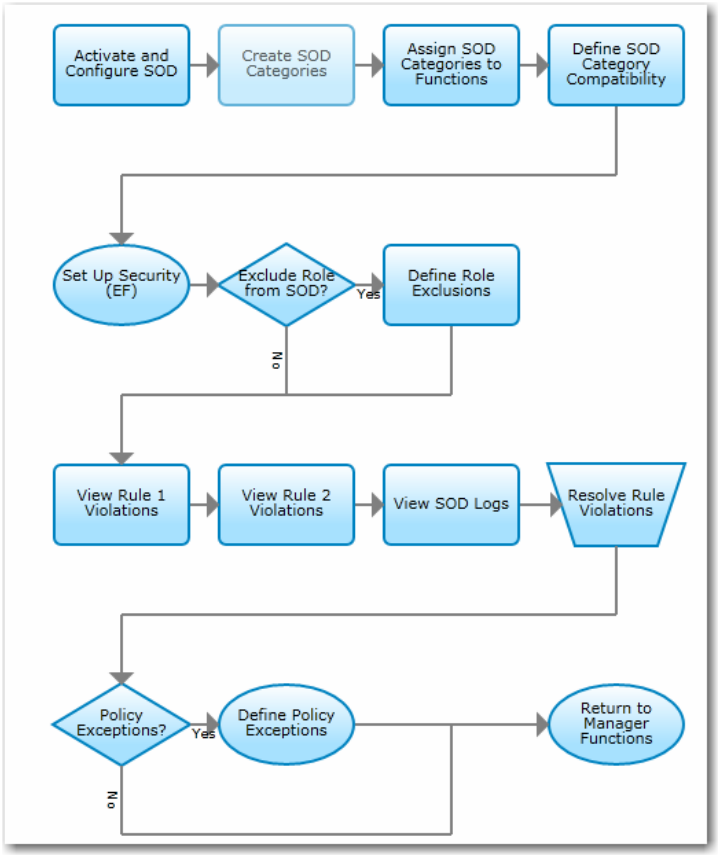
See “Maintain Segregation of Duties Policy Exceptions” on page 262.

Segregation of Duties Process Workflow

Important If your QAD Adaptive ERP system includes Adaptive UX, perform all segregation of duties setup in Adaptive UX. When you import the SOD Matrix of incompatible categories into Adaptive UX, Adaptive UX searches for conflicts across both Adaptive UX and Enterprise Edition resources. Currently, if you import the matrix through Adaptive ERP, only conflicts with Enterprise Edition resources are identified.

Use the options in the Segregation of Duties screens to set up segregation of duties and to configure segregation of duties functions. Figure 10.3 illustrates one possible segregation of duties process workflow; use it to set up segregation of duties functions in your environment.

Fig. 10.3
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 247. For details on planning and implementing security in your system, see “Implementation Summary” on page 6.

After you create user records and define roles in your system, the first activity is to activate segregation of duties using SOD Control and specify segregation of duties configuration settings. See “Activate Segregation of Duties” on page 255.

When segregation of duties is activated, you should then define the segregation of duties categories using SOD Categories. For each category, you specify a unique category code and a description. See “Maintain Segregation of Duties Categories” on page 256.

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. See “Define Role Permissions” on page 260.

Use SOD Categories 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 Segregation of Duties Categories” on page 256.

The next step is to define role permissions in your system. This associates application resources to user roles. See “Role Menus” on page 129. 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 Roles. See “Segregation of Duties Role Exclusions” on page 264.

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 Exceptions. See “Maintain Segregation of Duties Policy Exceptions” on page 262.

Use the SOD Violations Report and SOD Logs to view current segregation of duties policy violations and a violations history file. See “Report and View Logs and Violations” on page 272.

Segregation of duties violations that arise during segregation of duties maintenance are recorded in a log. Use SOD Logs Archive action to archive log table records. See “Archive Log Record Files” on page 275.

If who have default segregation of duties data ready to import into your system, you can use the Excel import and export functionality to more easily build your segregation of duties framework. See “SOD Setup” on page 264.

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 Services delivers a set of default roles and segregation of duties categories that facilitate the implementation of segregation of duties. You can load the provided segregation of duties data using Excel Import and Export on SOD Setup. See “SOD Setup” on page 264 for segregation of duties setup in Adaptive UX

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

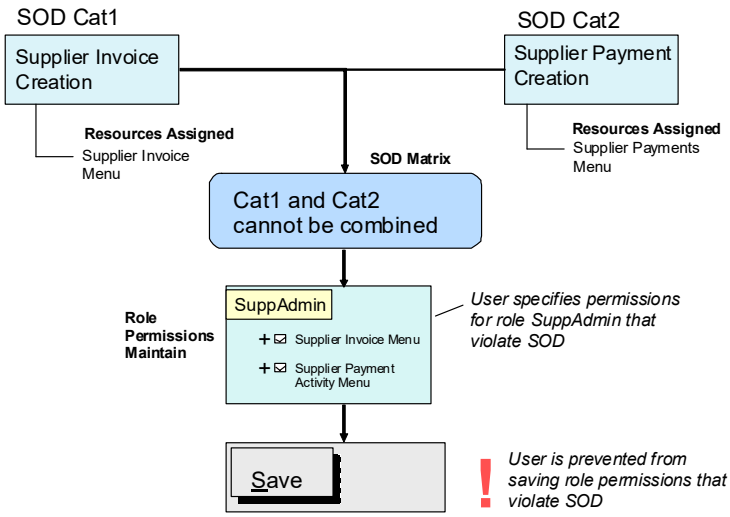
When you add a resource to the list of resources allowed for a role in Role Permissions, the system validates the assignment to verify that all the role resources belong to compatible segregation of duties categories (Rule 1 validation). If Rule 1 is violated, the system blocks the role permissions updates, 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 Block Violations checkbox is selected in SOD Control, the system blocks Rule 2 violations in Role Permissions 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. 10.4
Role Permissions Validation



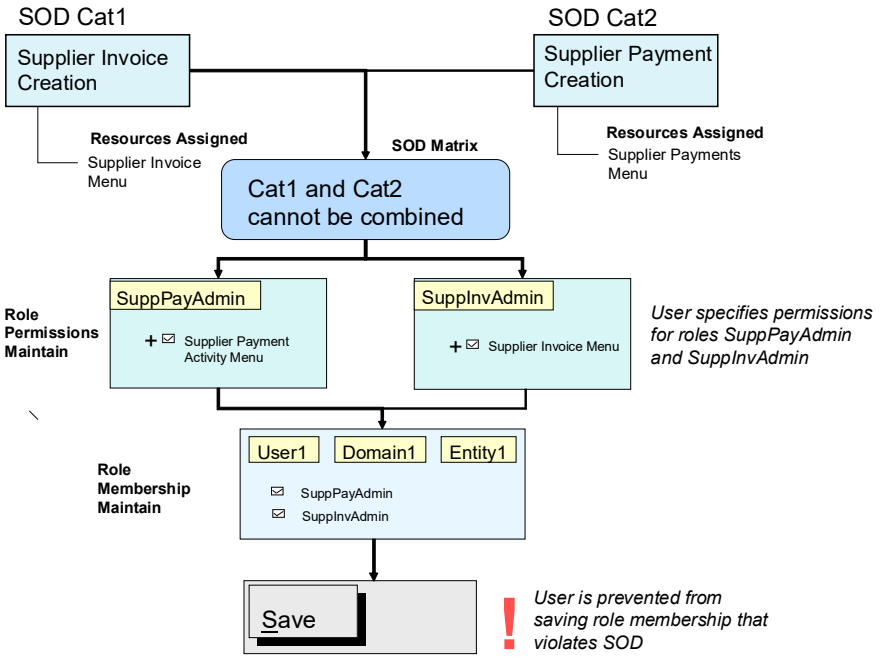
Role Membership Validation

When a user is added to a role using User Access, the system runs checks to validate that the roles to which the user belongs 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 Block Violations checkbox is selected in SOD Control, you are blocked from performing steps that violate role membership compatibility.

Fig. 10.5
Role Membership Validation



Direct and Indirect Violations

A direct segregation of duties violation occurs when you attempt to use Role Permissions to assign a role to functions that have incompatible segregation of duties categories. Direct violations also occur if you attempt to use User Access to assign multiple roles to a user that have incompatible segregation of duties categories.

Users are always blocked from performing actions in Role Permissions that cause Rule 1 violations and are always blocked from performing actions in User Access that cause Rule 2 violations, regardless of the setting in the Block Violations checkbox in SOD Control.

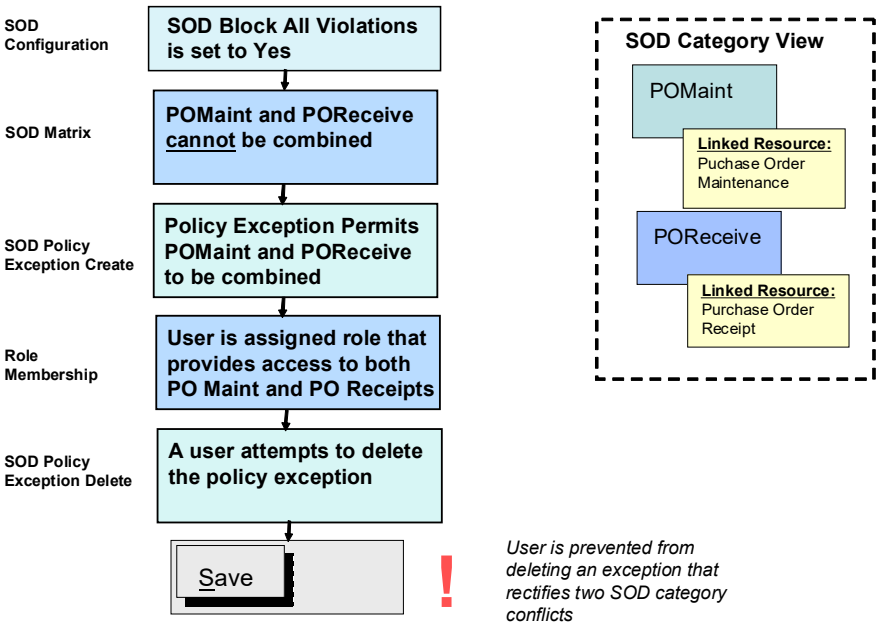
Indirect violations occur if you perform actions that violate segregation of duties rules using screens other than Role Permissions and User Access. However, role membership (Rule 2) violations caused by updates in Role Permissions are also examples of indirect violations.

Figure 10.6 shows how the system handles an indirect violation when the Block Violations field is selected in SOD Control. In this example, the segregation of duties category code POMaint applies to the creation of purchase orders (POs) in Purchase Orders, 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 Setup or SOD Categories.

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. 10.6
Indirect Segregation of Duties Violation



Segregation of Duties Rule Matrix

Table 10.1 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 10.1
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, 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.	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 User Access, 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 User Access.	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.	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 Categories.	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 Categories.	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 Exceptions 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 Exceptions. 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 the Exclude from SOD option on Roles 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 clear the Exclude from SOD field on Roles. 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 Control.	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 Control.	No segregation of duties checking.	Rule 1: Existing violations are fixed. Rule 2: Existing violations are fixed.	Not applicable.

Complete Prerequisite Activity

Ensure OpenEdge is using TLSv1.2. TLSv1.3 is not supported for segregation of duties. Enter the following settings in the `configuration.properties` file and then run `yab update`.

```
openedge.env.pscsslclient.key=PSC_SSLCLIENT_PROTOCOLS
openedge.env.pscsslclient.value=TLSv1.2
```

Before setting up segregation of duties, you must create user records in the system and provide basic identifying information. Use Users 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 104.

You also can define user roles—but not role permissions or role membership—as a prerequisite activity. See “Define Roles” on page 93.

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 Roles 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 Roles. 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 264.

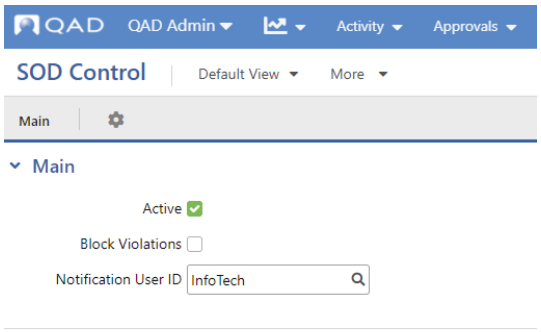
Important If you attempt to activate segregation of duties and the Excluded from SOD field is not selected for the SuperUser role, a warning displays to indicate that the activation may not process correctly.

Activate Segregation of Duties

Segregation of Duties can be activated from Adaptive UX, Adaptive ERP, and the command line. If your QAD system includes Adaptive UX, perform all segregation of duties setup in Adaptive UX. When you import the SOD Matrix of incompatible categories into Adaptive UX, Adaptive UX searches for conflicts across both Adaptive UX and Enterprise Edition resources. Currently, if you import the matrix through Adaptive ERP, only conflicts with Enterprise Edition resources are identified.

Use SOD Control to activate segregation of duties rule checking on your system.

Fig. 10.7
SOD Control



Active. Select the checkbox to activate rule checking for segregation of duties.

When you activate SOD, all validation rules are run to check for violations. You cannot continue implementing SOD if role permission (Rule 1) violations exist on your system. You must deactivate SOD, resolve the violations raised, and then re-implement SOD.

Note If the Block Violations checkbox is not selected, Rule 1 and Rule 2 violations are reported and SOD is activated; however, all Rule 1 violations must be resolved before you can start using SOD.

When you first begin to implement segregation of duties, it is recommended that you deactivate SOD rule checking, and only activate it again when you have defined all categories and incompatible categories, linked resources to segregation of duties categories, and defined roles. If you deactivate SOD, 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.

Block Violations. Select this checkbox if you want the system to block any changes to role-based security that would allow users to access conflicting resources. The effect of selecting Block Violations is that all indirect violations are blocked.

If this checkbox is not selected, administrators are not blocked from providing users with access to functions with conflicting segregation of duties categories.

Users are always blocked from performing actions in Role Permissions that cause Rule 1 violations and are always blocked from performing actions in User Access that cause Rule 2 violations. If you select this checkbox, however, the system also

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 Block Violations, the system checks if violations exist, and displays an error if violations are found. The checkbox cannot be selected until these violations are fixed.

If you leave the checkbox clear, 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 clear.

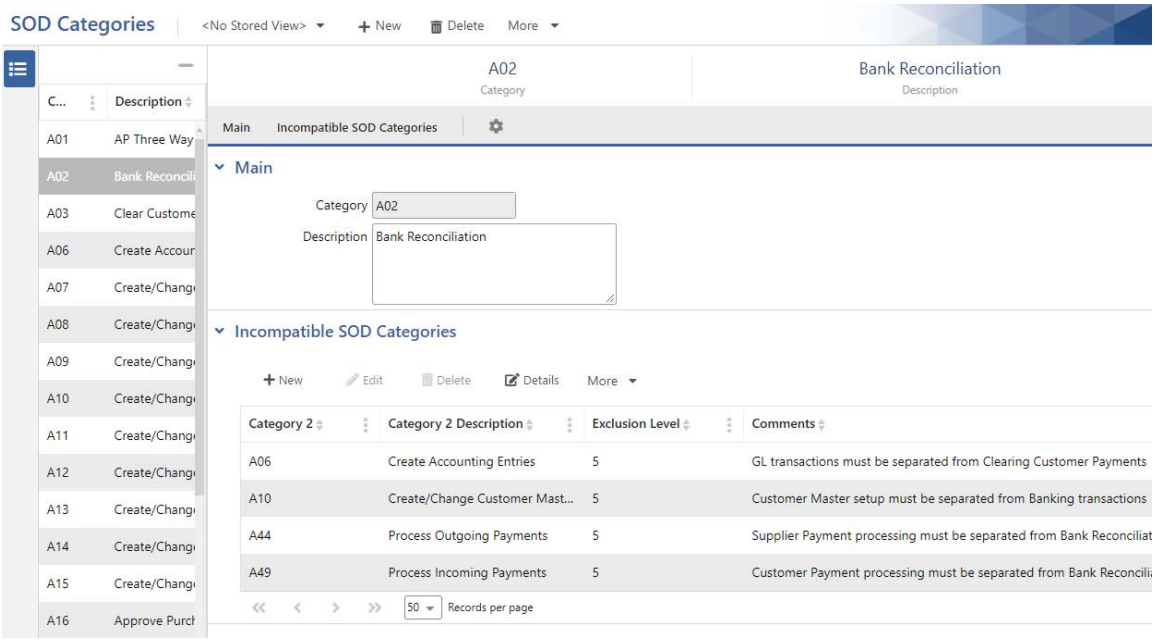
Notifications User ID. In addition to on-screen notifications and the SOD audit logs, the system can send notification of SOD violations to the User ID specified here. The notification can go to the user's external email address, the QAD inbox, or to both, depending on the Category Settings defined for Segregation of Duties on the user's Profile page.

Maintain Segregation of Duties Categories

Use SOD Categories to create, maintain, and delete segregation of duties categories. Add as many categories as required to accommodate your specific segregation of duties requirements.

SOD categories are used to group business activities that share similar characteristics within an organization. After defining your SOD categories, use the Incompatible SOD Categories grid to specify which categories are incompatible with each other.

Fig. 10.8
SOD Categories



Category. Enter a unique category name, with a maximum of 20 characters.

Description. Enter a description of the SOD category, with a maximum of 40 characters.

Incompatible SOD Categories

Category 2. Enter a category that is incompatible with the selected category.

Category 2 Description. The category's description.

Exclusion Level. Enter a value from 1 to 5 to associate a conflict level with the mutually exclusive categories. Use this optional setting to set up better filtering capabilities for SOD reports.

Comments. Enter text to explain why the two categories are mutually exclusive.

Assign Resources to Segregation of Duties Categories

Use SOD Category Membership 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 Categories. Then specify the category incompatibilities in SOD Categories.

You select resources to assign to categories using a tree view similar to that in Role Permissions. 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.

Assigning Resources

Resource types that are eligible for segregation of duties are:

- Business Components
- Services
- Reports
- Field Groups

Resource types that are not eligible for SOD are:

- Apps
- Browses
- Dashboards
- Fields
- KPIs
- Links
- Views

Every application resource has one or more permission types, such as read and create. A resource's permission types can each be assigned to one and only one SOD category or no SOD category, and the resource's permission types can each have a different SOD category from the others.

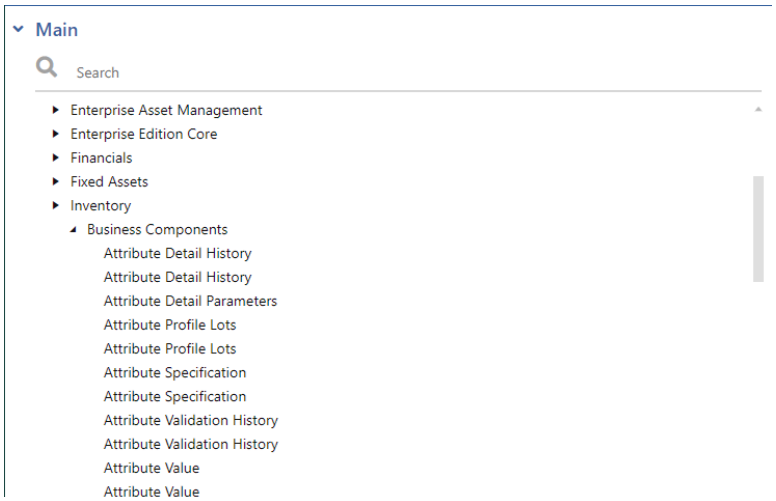
- If associated with a category, the resource's permission type is only compatible with other resource permission types that are associated with a compatible SOD category, with resource permission types in the same SOD category, and with permission types that are not assigned to an SOD category.
- If associated with no category, the resource is compatible with any other application resource, regardless of the SOD category to which those resources may be attached.

Use the resource tree to select a resource and then use the Default SOD Category lookup and the Permission types grid to assign category membership.

Resource Tree

The resource tree identifies how resources are organized in the system in a hierarchical manner.

Fig. 10.9
Adaptive UX Resource Tree



Select a resource to make it the active option in the right-hand panel.

Resource Tree Search

You can search for resources by label name or URI using the Search feature at the top of the resource hierarchy tree. Search results display the resource type icon to the left of the search list items and partial URIs to the right side of the search list items. You can select a search result and edit the resource's category membership in the right-hand panel.

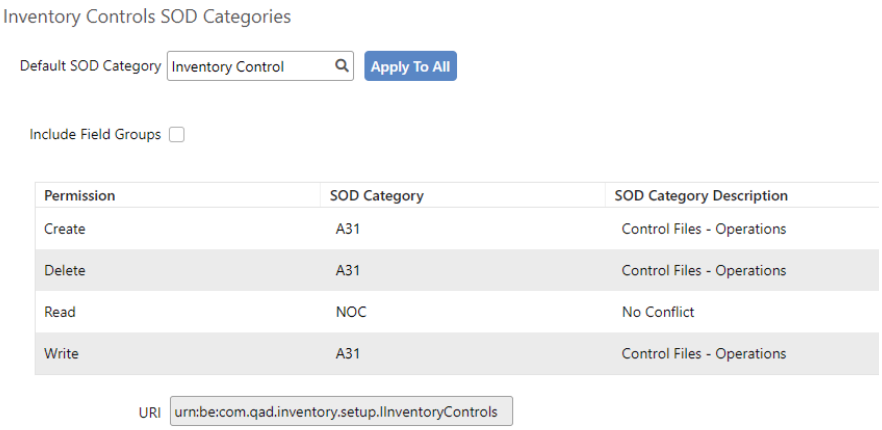
If you need more information to determine which result is the correct resource, you can view the resources within the context of the hierarchy.

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

SOD Categories and Permissions Grid

The right side of SOD Category Membership contains the default SOD Category field and a permission types grid. Use the Apply to All button to assign the default SOD category to all permission types of the secure resource and then update the individual permission types within the grid as needed.

Fig. 10.10
Adaptive UX Permissions Grid



Include Field Groups. Select this checkbox when a business component's field groups need to be included in segregation of duties violation checks. When selected, the treeview on the left side of the screen expands to display the field groups for the selected business component. Configure the SOD categories for the field groups as needed.

Note If the business component does not include any field groups, selecting the checkbox has no effect on the resource tree.

Permission. The permission types associated with this application resource.

SOD Category. The SOD category assigned to the permission type. You can edit the SOD Category field for each permission type independently by selecting the field in the grid.

SOD Category Description. The SOD category's associated description.

The URI is provided for informational purposes.

When you select Save, the system validates that the new SOD category assignments do not conflict with existing settings. Depending on settings defined during SOD configuration, the system blocks the save or saves the settings and logs the conflict in SOD Logs.

Define Role Permissions

Use Role Permissions 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 101 for details on this function.

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 Categories to maintain the compatibility of segregation of duties categories. See “SOD Categories” on page 265.

If a user needs to be assigned to more than one role, the roles must be compatible with each other, or there must be a policy exception that exempts any incompatible pair of roles.

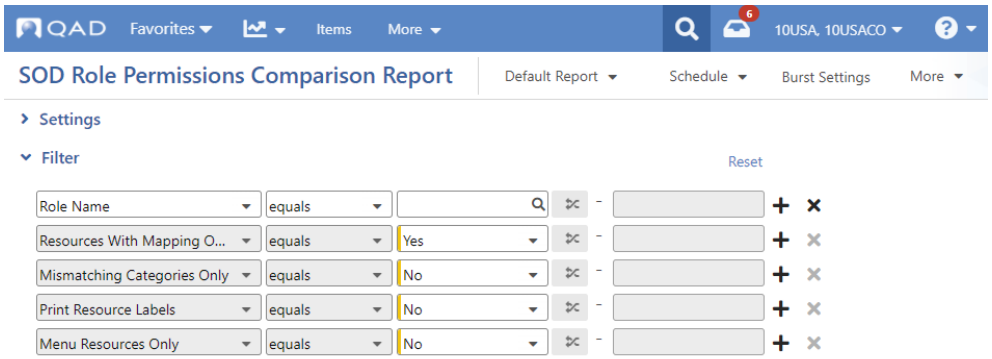
If you try to assign a user to a role that is incompatible with one or more of the roles already assigned to the user, when you attempt to update the database the system displays an error and does not assign the role.

When a user is restricted from using an application resource, the user cannot access the resource by typing its name.

SOD Role Permissions Comparison Report

The SOD Role Permissions Comparison Report simplifies synchronizing role permission settings between Enterprise Edition and Adaptive UX by mapping Enterprise Edition resources to their equivalent Adaptive UX resources.

Fig. 10.11
SOD Role Permissions Comparison Report



The filters affect the report output in the following ways:

Role Name. This filter allows you to select a single role or view all roles by clicking the X to remove Role Name as a filter.

Resources With Mapping Only. This filter returns the EE Resource URI and its corresponding SOD category, the associated Adaptive UX Resource URI and its corresponding SOD category, and the assigned permission type.

Mismatching Categories Only. This filter removes the EE and Adaptive UX resources that are identical and shows only those resources that have different SOD categories in Enterprise Edition and Adaptive UX.

Print Resource Labels. This filter replaces the resource URI with menu titles for Enterprise Edition and resource labels for Adaptive UX.

Menu Resource Only. This filter returns the mapping of Enterprise Edition resources to menu-eligible resources in Adaptive UX. Menu-eligible resources, such as views, can belong to business components, which themselves can have multiple permission types. If multiple SOD categories are assigned to a business component and not to the view, those categories are listed in the SOD Category column as comma-separated entries.

Define Role Membership

Use User Access 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 119.

Maintain Segregation of Duties Policy Exceptions

Use SOD Policy Exceptions 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.

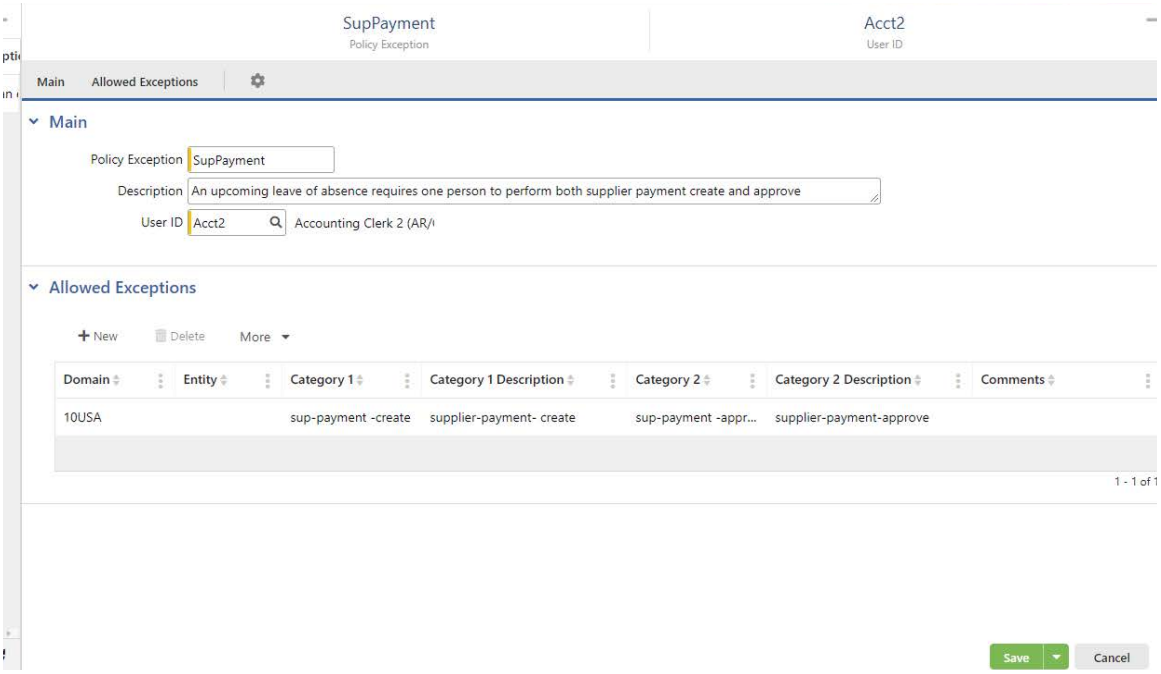
Policies are checked any time a change is made that impacts segregation of duties; for example, when a user is assigned to a role, when you link resources to categories, when you change role permissions, or when you change role membership.

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.

SOD Policy Exceptions

You can create, maintain, and delete policy exceptions on the SOD Policy Exceptions screen.

Fig. 10.12
SOD Policy Exceptions



In the Main panel, define the policy exception.

Policy Exception. Enter a policy exception code.

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 (management controls that are outside the system) that your organization uses to mitigate risks arising from the exception.

User ID. Enter a user ID to identify the user to whom this policy exception applies.

In the Allowed Exceptions panel, specify if the exception applies to the whole system, a domain, or a single entity and the incompatible categories that this exception will allow for the specified user ID.

Domain. Specify a domain in which this policy exception applies. When a domain is selected, the policy exception applies to all entities in the domain.

Entity. If a domain has not been selected, you can specify an entity in which this policy exception applies for the selected user ID. If a domain is selected, the policy exception applies to all entities in the domain and the entity field is disabled.

Category 1. Specify the first category in the pair for which this exception applies. If you use the lookup, which displays the SOD Matrix, to select a category, the Category 2 field defaults to the associated incompatible category.

Category 1 Description. Enter a description of Category 1.

Category 2. Specify the second category in the pair for which this exception applies. If you selected the first category using the lookup, this second segregation of duties category defaults automatically.

Category 2 Description. Enter a description of Category 2.

Comments. Enter a detailed description of why the policy exception is required for the segregation of duties categories. This field is optional.

The system validates entries in the required fields as you enter them.

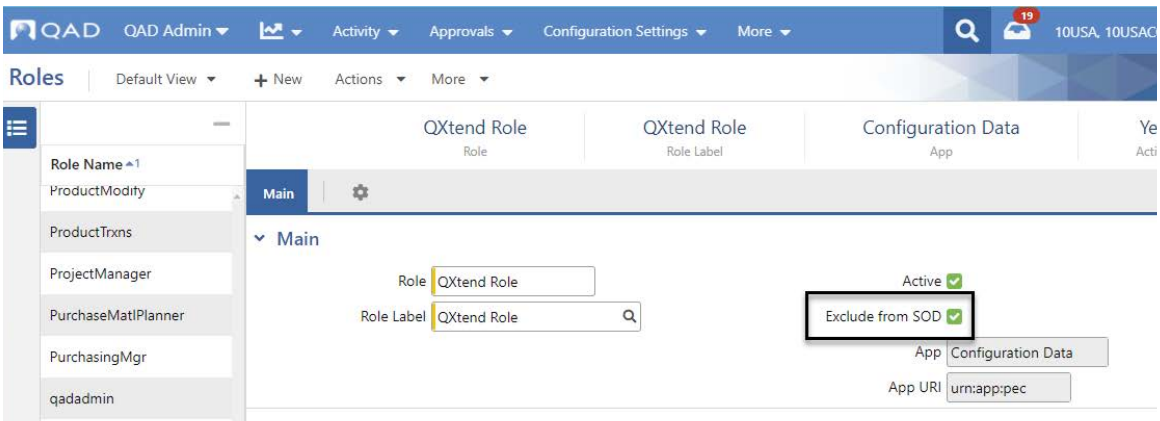
Segregation of Duties Role Exclusions

You can specify particular roles to be 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 and sparingly.

This exemption is set on the Roles screen, as shown in Figure 10.13, or from the Roles grid on SOD Setup. When the Exclude from SOD checkbox is selected, the role is excluded from segregation of duties Rule 1 and Rule 2 validations. See “Create a New Adaptive UX Role” on page 95 for details on creating new roles.

Fig. 10.13
Exclude from SOD



SOD Setup

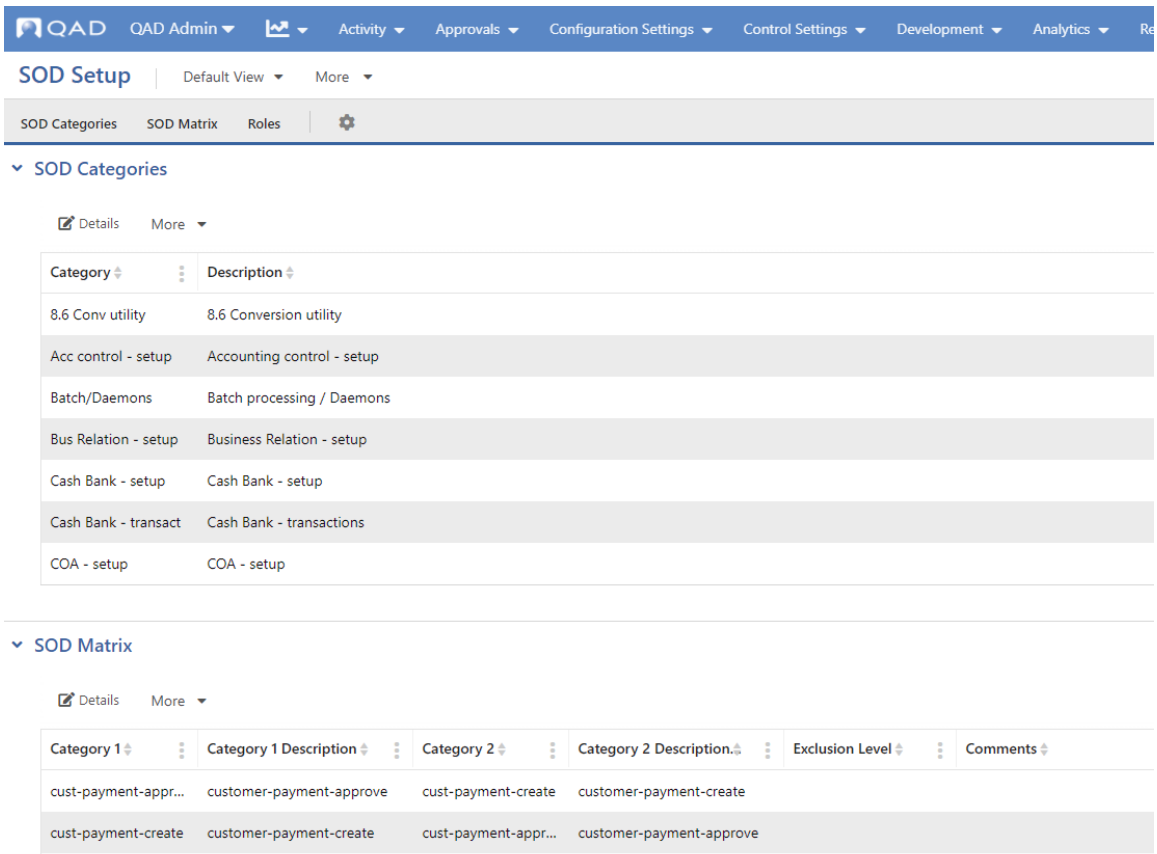
SOD Setup brings together SOD categories, the SOD matrix of incompatible categories, and system roles. From this screen, you can load default data for segregation of duties categories, matrices, menus, resource assignments, and roles using a single Excel spreadsheet. The import function lets you check for role permission (Rule 1) and role membership (Rule 2) violations before saving the data to the database.

QAD provides default segregation of duties data to use during the deployment process. This default data is based on best practices, and has not been validated by an external audit company.

Note If you reload the default data after you have modified segregation of duties content in the environment, the reloaded default data will overwrite the modifications and restore the SOD categories and matrix settings to those defined in the default data.

You can export and import your environment's segregation of duties data to an Excel file to add and update settings as well as to move it from one environment to another. See "Import and Export Segregation of Duties Data" on page 267 for more information on Excel integration.

Fig. 10.14
SOD Setup



SOD Categories

The SOD Categories grid lists all of the segregation of duties categories as they appear on the SOD Categories screen. Highlight a category and click Details to view a category's associated incompatible categories and add new incompatible categories as needed.

Category. The unique category name.

Description. The description of the category.

SOD Matrix

The SOD Matrix grid lists all pairings of incompatible categories. This information can be found in filtered form on the individual SOD Categories screen for every category.

Category 1. A segregation of duties category that is not compatible with the entry in Category 2.

Category 1 Description. The description of the entry in Category 1.

Category 2. A segregation of duties category that is not compatible with the entry in Category 1.

Category 2 Description. The description of the entry in Category 2.

Exclusion Level. This value, from 1 to 5, associates a conflict level with the categories. Use this optional setting to set up better filtering capabilities for segregation of duties reports.

Comments. Information that explains why the two categories are incompatible.

Adding a New Incompatible Categories Pairing

To add a new incompatible categories pairing, one of the categories already must be listed in the Category 1 column in the matrix. If one of the incompatible categories is not listed as Category 1, go to the SOD Categories screen to create the pairing.

1. Highlight the Category 1 record that requires another incompatible category. Click Details to view the individual record.
2. From the detail view, click New.
3. Select or enter a new incompatible category in the Category 2 field.
4. Optionally, enter an exclusion level and comments.
5. Click Save to create the new incompatible category record.

Roles

The Roles grid lists all of the roles as they appear on the Roles screen. Highlight a role and click Details to update its current settings.

Role. The role name.

Role Label. The role label.

Active. When selected, the role is active in the system upon save.

Exclude from SOD. When selected, the role is excluded from segregation of duties Rule 1 and Rule 2 validations.

Import and Export Segregation of Duties Data

On the SOD Setup screen, the Import and Export options in the More menu let you create and load default data for segregation of duties categories, matrices, role menus, 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. The Excel spreadsheet you export contains the following worksheets:

- SOD Category
- SOD Matrix
- Menu
- Resource
- Resource Property
- Role

If you export just the template from your system, the sheets have column headers but no data. If you export with your system data, the sheets are populated with their respective details.

SOD Category

The SOD Category sheet lists all of the categories and their associated descriptions. You can add new categories and edit existing category descriptions. 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. If you delete a category from the sheet, it will not be deleted from the system upon import.

SOD Matrix

The SOD Matrix sheet has five columns:

- SOD Category 1
- SOD Category 2
- Cannot be combined with
- Level
- Comments

The sheet lists all possible combinations of existing categories, both compatible and incompatible. You can edit existing combinations and add new combinations for import into the system. If you delete a row, that change will not be reflected in the system upon import.

Category combinations that are compatible have an entry of FALSE in the “Cannot be combined with” column and do not appear in the Adaptive UX SOD Matrix grid. Category combinations that are incompatible have TRUE in the “Cannot be combined with” column and are listed in the SOD Matrix grid in Adaptive UX. The Level column is for an optional value, from 1 to 5, that can be used for filtering on SOD reports.

Menu

The Menu sheet has five columns:

- Menu Type
- Menu Code
- Path
- Resource URI
- String Code
- Primary Secure URI
- Include In Mobile

The sheet represents role menus, with each row corresponding to a single menu item of a role menu. Menu Type is always Role, because Favorites menus are not supported as part of the export and import process.

Role menus in the system with no menu items are not exported, meaning menus must have pages and/or folders assigned to them to be included on the sheet.

The Menu sheet is synced with the Role sheet. Upon export, the Menu sheet only contains data related to roles listed on the Role sheet. During import, the system only loads menu data related to roles on the Role sheet and ignores other entries.

Resource

The Resource sheet has four columns:

- Resource URI
- Resource Label
- Permission Type
- SOD Category

The sheet identifies the resources and permissions assigned to a segregation of duties category. You can assign a category to a resource, change the category assigned to a resource, or clear the SOD Category field to remove a resource and category assignment.

Adaptive UX resources can have multiple permissions assigned to them, such as Read, Create, and Delete. Because of this permission granularity, one Adaptive UX resource can be listed multiple times for the same category on the Resource sheet, with each permission type having its own row.

The Resource sheet is synced with the Role sheet. Upon export, the Resource sheet only contains data related to roles listed on the Role sheet. During import, the system only loads resource data related to roles on the Role sheet and ignores other entries.

Resource Property

The Resource Property sheet has three columns:

- Resource URI

- Property Name
- Property Value

The data on this sheet represent resource properties. This includes properties such as “IncludeFieldGroups,” which shows that a resource includes field groups in segregation of duties processing.

Role

The Role sheet has four columns:

- Role Name
- Role Description
- Active
- Exclude from SOD

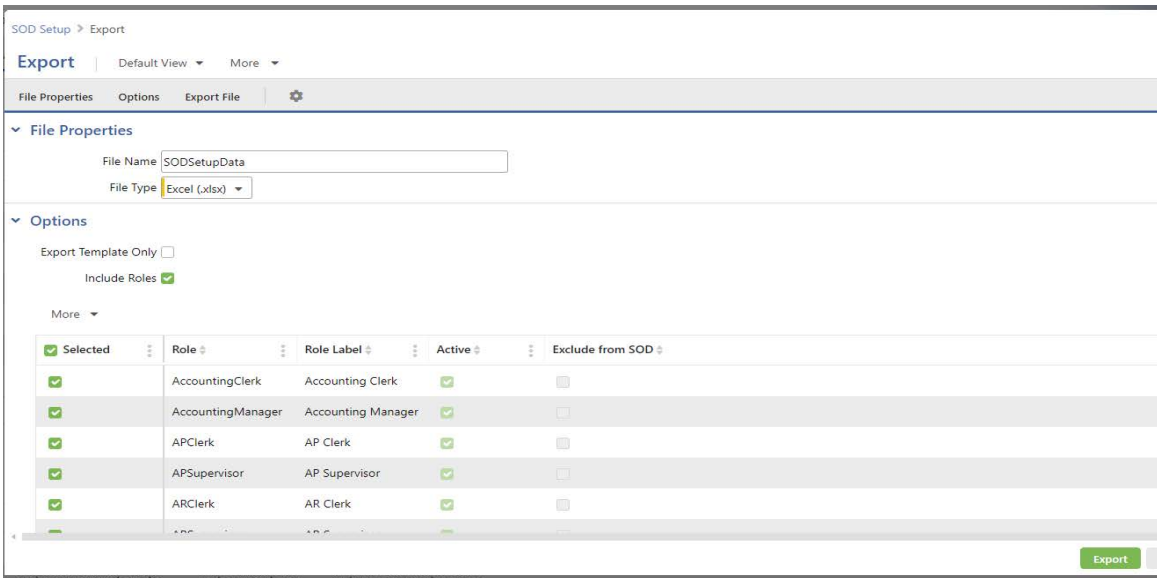
The Role sheet lists the roles that were selected during export, if any. You can edit existing roles and add new roles to be included in the system when the file is imported. For each role, you can indicate if the role is active or inactive, and indicate if any roles are excluded from segregation of duties limitations. If you delete a role from the sheet, that change will not be reflected in the system upon import.

The Role sheet is synced with the Menu and Resource sheets. Upon export, the Menu and Resource sheets only contain data related to roles listed on the Role sheet. During import, the system only loads menu and resource data related to roles on the Role sheet and ignores any other entries.

Export to Excel from SOD Setup

Choose More > Export to create an Excel file in the format required for reloading data to the system. You can save the exported file to your local drive to make updates before importing your additions and revisions.

Fig. 10.15
SOD Setup Export



On the Export screen, fill out the following fields to define the structure of the exported file.

File Properties

File Name. Enter a name for the file being created by the export action.

File Type. Select the file type. Currently, you can only export to an Excel (.xlsx) file.

Options

Export Template Only. When selected, the Export action does not include data in the exported Excel file. The template contains all predefined sheets and each sheet's default columns. The default sheets contain the following columns.

- SOD Category contains Category and Description.
- SOD Matrix contains SOD Category 1, SOD Category 2, Cannot be combined with, Level, and Comments.
- Menu contains Menu Type, Menu Code, Path, Resource URI, String Code, Primary Secure URI, and Include in Mobile.
- Resource contains Resource URI, Resource Label, Permission Type, and SOD Category.
- Resource Property contains Resource URI, Property Name, and Property Value.
- Role contains Role Name, Role Description, Active, and Exclude from SOD.

Include Roles. When selected, a grid appears, as shown in Figure 10.15, that displays all system roles in the Options panel. Select which roles and their associated data to include in the exported file.

Export File

Results will be sent to your inbox. After you define how you want the exported file to appear, click Export to generate the Excel file.

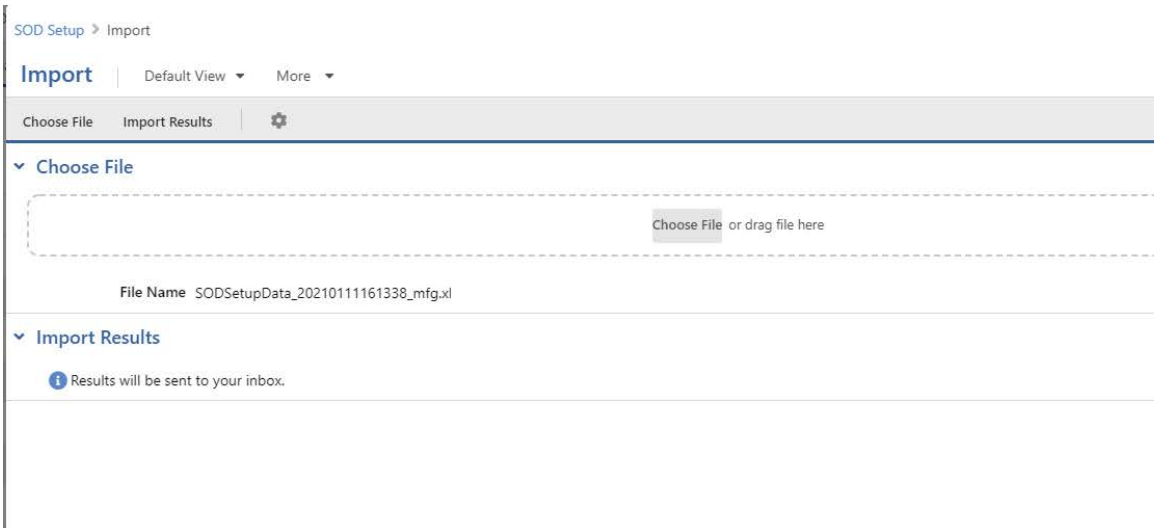
Import to SOD Setup

The Menu and Resource sheets are synced with the Role sheet and the system only loads menu and resource data related to roles on the Role sheet. Menus and resources are imported using the replace method, which means menus and resources already in the environment that have valid entries on these two sheets are deleted and the new data is imported. This ensures the import does not result in an unexpected mix of menu items and role permissions for the imported roles.

All other sheets are imported using the append method. If no data existed in the system before the import, it is created. If data existed, the import adds to the existing entries and does not overwrite or delete settings.

Choose More > Import to import a modified Excel spreadsheet containing segregation of duties data.

Fig. 10.16
SOD Setup Import



Choose File

Select the file to import using the Choose File button or by dragging the file into the highlighted box. The system validates the file structure and checks for Rule 1 and Rule 2 violations as the file is uploaded and any violations are displayed in the SOD Violations panel. All Rule 1 conflicts must be resolved before the file can be imported.

If the Excel file has invalid entries, those lines of the file are skipped and all valid entries will be imported.

Import Results

Once the file loads successfully, click Import. The results of the upload are sent to your inbox.

Report and View Logs and Violations

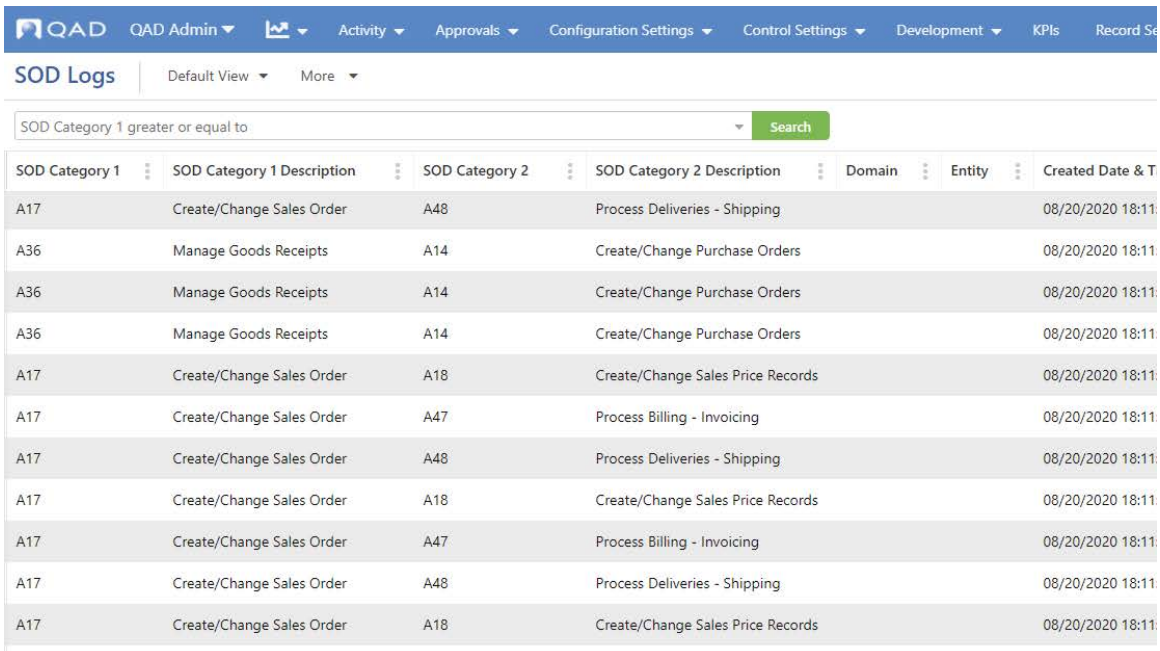
View Log History

The SOD Logs 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 includes:

- 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. 10.17
SOD Logs



Report on Current Segregation of Duties Conflicts

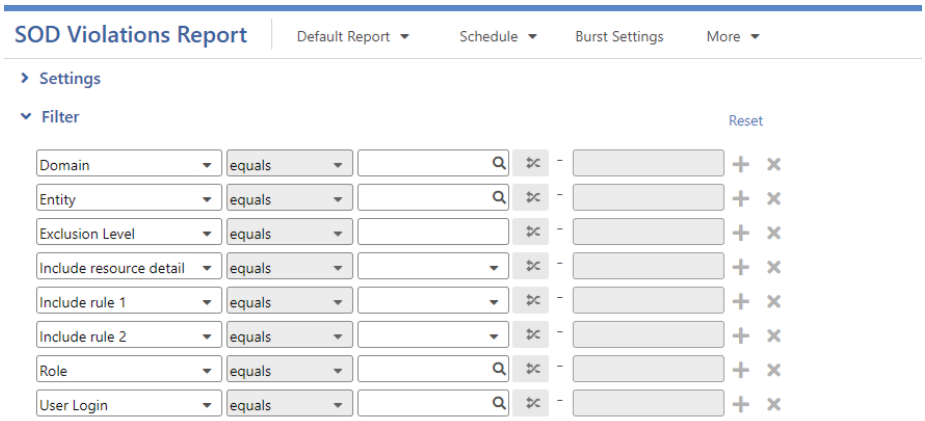
Use the SOD Violations report to determine whether there are compliance violations for role permissions, role membership, or both in the system.

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 10.18 illustrates the selection criteria for the SOD Violations report.

Fig. 10.18
SOD Violation Report, Selection Criteria



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 Violations report 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

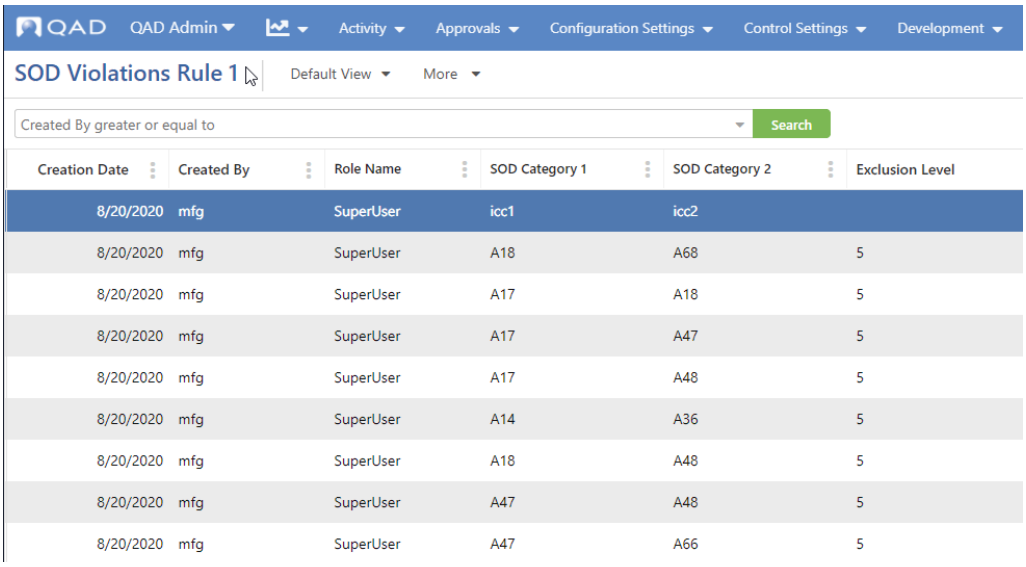
Category codes are displayed with their description. Resources are displayed with their corresponding menu entry and label.

Fig. 10.19
SOD Violations Report

View Role Permissions Violations

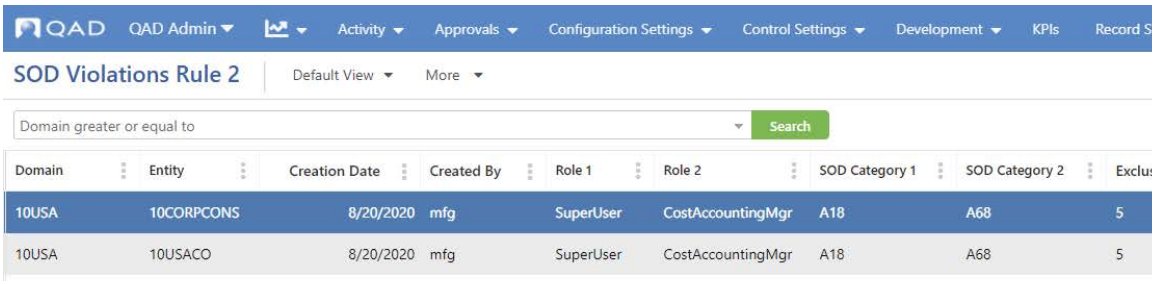
Use SOD Violations Rule 1 to display details of role permission violations.

Fig. 10.20
SOD Violations Rule 1



Use SOD Violations Rule 2 to display details of role membership violations.

Fig. 10.21
SOD Violations Rule 2



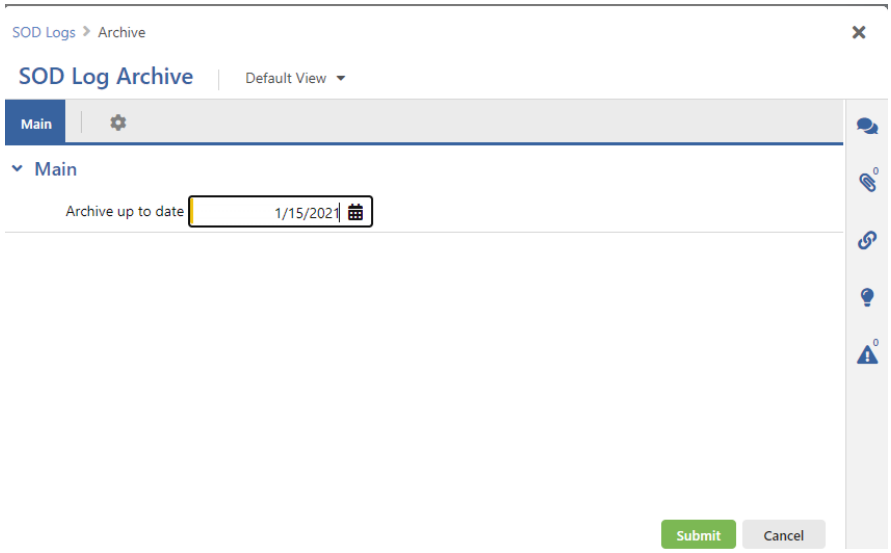
Archive Log Record Files

Use the Archive action on SOD Logs 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 SOD Logs.

When implementing security in your system, you should restrict access to this program.

Fig. 10.22
SOD Log Archive



Archive Up to Date. Select the date before which all records will be archived and removed from the SOD Logs screen.

Chapter 11

Electronic Signatures in Adaptive ERP

This section discusses how to set up and use electronic signatures functionality in your system.

Overview 278
Explains the purpose of the electronic signature features, lists eligible programs, describes the planning steps when implementing electronic signatures, illustrates the electronic signatures workflow, and explains QAD-specified categories, tables, and fields.

Set Up Electronic Signature Functionality 283
Explains the steps necessary to set up records that control when electronic signatures are recorded.

Electronic Signature Categories 285
Describes electronic signature categories and the category considerations, tables, fields, and filters.

Electronic Signature Profiles 291
Describes electronic signature profiles and lists the steps required to set up and use electronic signature profiles.

Record Electronic Signatures 300
Describes how electronic signatures are processed through the system with details on transaction scoping and product change control.

Email Notifications 303
Explains how and when the system generates and sends emails to system users and lists the different types of notifications.

Reporting 304
Lists the areas through which reports and inquiries are available and gives details about each type.

Archive and Restore Records 309
Describes how to use E-Signature Archive/Delete to archive electronic 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 electronic signatures can be used to support automated processing.

The electronic signature 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 101.

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.

Important Electronic signatures can be enabled in Adaptive ERP and Adaptive UX, and operate in both user interfaces simultaneously. However, you must set up and configure the functionality in both UIs separately. In addition, as you enable electronic signature configurations in Adaptive UX, you should disable the related functionality in .NET by removing permissions to menu options. This ensures reports and histories for electronic signature events are confined to one interface with a consistent reporting structure. Contact QAD Support for assistance with Adaptive UX electronic signature configuration.

Electronic Signature Enabled Programs

Electronic 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 288. Table 11.1 lists the programs that currently can have electronic signatures enabled.

Table 11.1
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

Module	Menu	Program
Regulatory Attributes	1.22.1	Lot Master Maintenance
	1.22.2	Lot Master Inquiry
	1.22.24	Regulatory Attributes Control
Inventory Control	3.1.1	Inventory Detail Maintenance
	3.1.2	Detail Maintenance by Item/Lot
	3.4.1	Transfer–Single Item
	3.4.3	Transfer With Lot/Serial Change
	3.4.4	Batchload Transfer with Lot/Serial Change
	3.6.5	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
	16.20.13.15	Operations By Employee Report
Item Attributes and Quality Control	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

Module	Menu	Program
	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
	19.26.13	QM Test Results Maintenance
	19.26.15	QM Test Results Report
	19.26.20	QM Certificate of Analysis Print
Master Data Reports	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 308.

The electronic signature function prompts for and maintains signature information based on signature profiles. Each profile is associated with a specific category of data and indicates whether signatures should be captured and for which menu programs, as well as which fields are being signed.

Important Categories are defined by QAD and delivered with the electronic signature functionality. Adding new categories requires custom development.

Programs for Electronic Signature Setup and Reporting

Table 11.2 shows the programs available for setting up and reporting on electronic signature functions.

Table 11.2
Electronic Signatures Programs

Menu Number	Description	Program Name
36.12.4	E-Signature Events Report	esevtrp.p
36.12.5	E-Signature History Report	eshstrp.p
36.12.7	E-Signature Failure Report	esflrp.p
36.12.14.1	E-Signature Group Maintenance	escgmt.p
36.12.14.2	E-Signature Group Report	esgrrp.p
36.12.14.4	E-Signature Workbench Refresh	eswpref.p
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

Electronic Signature Planning Steps

Before electronic signature processing can begin, the prerequisite planning steps must be completed.

The first activity in setting up electronic 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 Adaptive Applications fits into your overall business processes, as well as which specific electronic signatures support those processes.
- Complete data mapping requirements for records and available signatures.
- Determine 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.

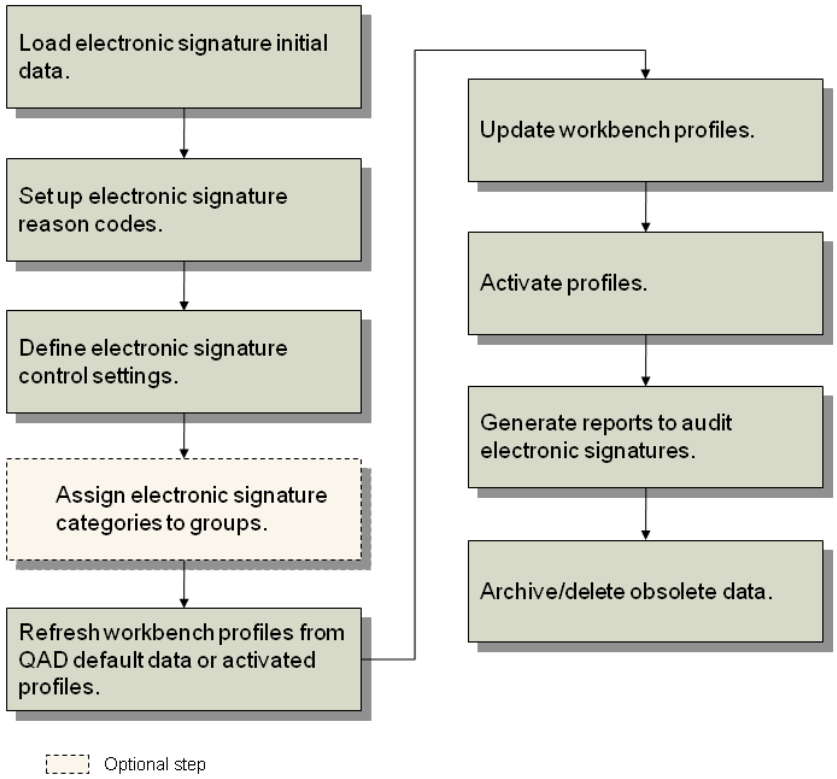
  Note Electronic signatures should be part of a detailed security plan to meet your overall business requirements.

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.

Electronic Signature Workflow

The following electronic signature workflow can be used to set up electronic signature functions in your environment.

Fig. 11.1
Electronic Signatures Workflow



1. **Load electronic 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 Electronic Signature Initial Data” on page 283.

2. **Set up electronic signature reason codes.** Electronic 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 electronic signatures must have an “ESIG” reason type. See “Set Up Electronic Signature Reason Codes” on page 283.

3. **Define electronic signature control settings.** When setting up electronic 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 284.

4. **Optionally, assign electronic signature categories to groups.** Optionally, define electronic 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 “Electronic Signature Categories” on page 285.

5. **Refresh workbench profiles from QAD default data or activated profiles.** See “Refresh Signature Profiles” on page 293.

6 **Update workbench profiles.** When initially setting up electronic signature functions, workbench category profiles are empty and must be manually populated. Use E-Signature Workbench Refresh (36.12.14.4) to update the empty profiles with the QAD-provided default information. You can refresh one category at a time or, optionally, refresh the profiles for an entire group of categories. See “Refresh Profile Frame” on page 294

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 electronic 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 Electronic Signature Profiles” on page 299.

8 **Generate reports to audit electronic signatures.** Use E-Signature Events Report (36.12.4) and E-Signature History Report (36.12.5) to view information that applies to electronic signatures. Use E-Signature Failure Report (36.12.7) as part of your security program to identify potential unauthorized access attempts. See “Electronic Signature Records for Quality Control” on page 305.

9 **Archive/delete obsolete data.** Use E-Signature Archive/Delete (36.12.14.22) to archive electronic 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 309

Set Up Electronic Signature Functionality

When setting up electronic signature functionality, the following tasks must be completed:

- Load Electronic Signature Initial Data
- Set Up Electronic Signature Reason Codes
- Define Security Control Settings

Load Electronic 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 Electronic Signature Reason Codes

The signature reason code is a critical element of the electronic signature. In regulatory environments, the signature record typically must include the meaning of the signature. The system uses reason codes to provide the meaning.

Each time the system prompts for an electronic signature, the user must provide a valid reason code. For example, reason codes might indicate that a quality record has been approved, reviewed, or inspected. See “Record Electronic Signatures” on page 300.

Use Reason Codes Maintenance (36.2.17) to define signature reason codes that are appropriate to your environment.

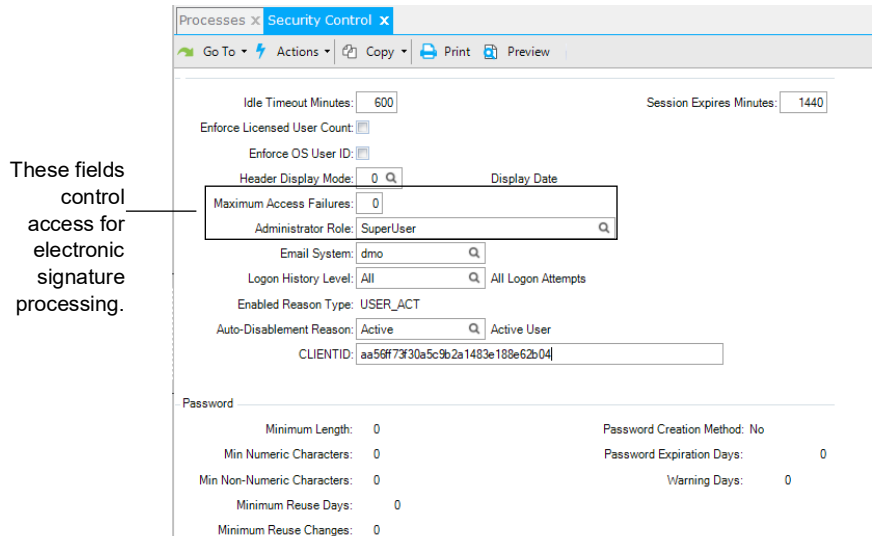
Important All reason codes used by electronic signatures must be associated with the QAD-provided ESIG reason type. Reasons of any other type cannot be entered in the signature prompt frame.

Define Security Control Settings

To prevent any unauthorized individuals from applying electronic signatures using another user’s ID, electronic 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 electronic 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. 11.2
Security Control (36.3.24)



Two fields directly control how the system manages unsuccessful electronic 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 email when a session is terminated because of excessive unsuccessful signature attempts. The system also sends email to users who are assigned this role when a signature profile is activated. See “Email Notifications” on page 303.

Electronic 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 289.

Table 11.3 lists the electronic signature categories, as well as the default menu programs associated with them. If you do not want a particular program to generate electronic signatures, you can clear its selection in the workbench profile. See “Apply Profile to Menu Programs” on page 298.

Table 11.3
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)

Code	Name	Description	Available Menu Programs
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)
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

Code	Name	Description	Available Menu Programs
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 electronic signature data. See “Functional Reports and Inquiries” on page 308 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 electronic signature when you access a previously signed record from one of the programs listed in Table 11.3 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 Electronic Signatures” on page 300.

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 electronic signatures occur. This section outlines the effects of auditing and signing temporary location detail records (ld_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 ld_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 ld_det record

- One to create it with all new values
- One to update the QOH

The delete event is for a different ld_det record than the create and modify.

When electronic 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 electronic signatures on this type of record.

Tables and Fields

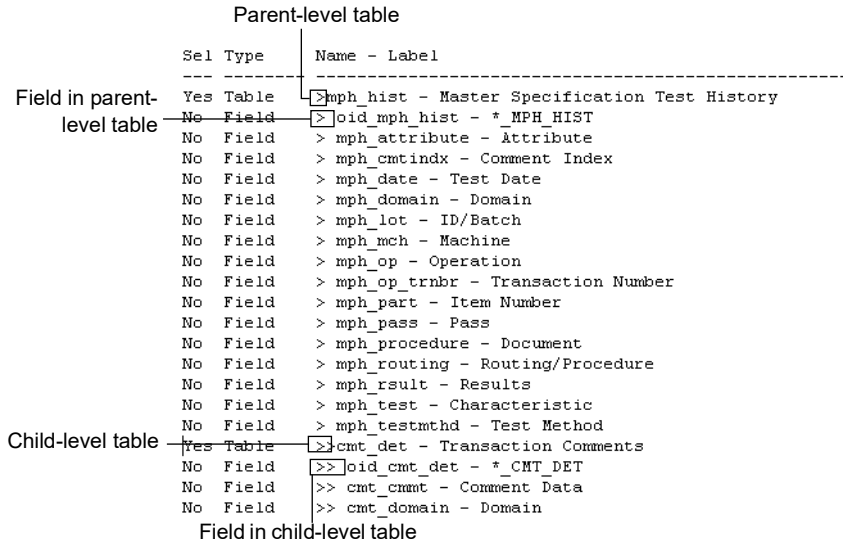
The category profile includes a list of tables and fields that define the data to be signed in the corresponding signature-enabled programs. See “Update Signature Profiles” on page 295.

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 11.3 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. 11.3
Example of Workbench Profile Table/Field Structure



Top Tables

Each QAD-provided category definition includes a top-level table, which displays in the Top Table field in the first frame of E-Sig Workbench Profile Maintenance. In most cases, this is the first table that appears in the profile structure.

In other cases, however, the top table is not included in the data to be signed but instead provides key values for identifying the signed data.

Example The top table in the Quality Results category is the work order routing (wr_route) table, but this table is not included in the data to be signed; that consists of the master specification history (mph_hist) table and related transaction comments (cmt_det). The wr_route record is used only to identify the signed data by providing the context.

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 “Electronic Signature Reports” on page 305.

Filters

Depending on the specific requirements of your environment, you may not need to record electronic signatures for all records of a given type. For example, you might want to require signatures only on inventory transactions involving a specific site or certain items.

QAD-provided categories include filters for selecting or excluding data that must have electronic signatures applied.

Table 11.4 indicates the filters that are available in each QAD-provided category definition.

Table 11.4
Available Filters, by Category

	Filter				
Category	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 299.

Filters are designed to work either by inclusion or exclusion, as defined by the Filter Mode field in E-Signature Workbench Profile Maintenance. For example, an *inclusion* filter might be set up to include records by site and location. If you set up the filter criteria with site values of 1000 and 2000 and location values of loc1 and loc2, only records with a combination of one of those sites and one of those locations will require an electronic signature. In this scenario, updating a record associated with site 1000, loc3 would not trigger a prompt for an electronic signature.

In the same example, defined as an *exclusion* filter, electronic signatures would not be required for records with any combination of the specified sites and locations. Updates to records with any other sites and locations, however, would trigger a signature prompt.

A profile can have either inclusion or exclusion filters, but not both.

Electronic Signature Profiles

Overview

The electronic 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 electronic signatures are required
- In which programs
- Which fields are signed
- Characteristics of how signatures are displayed and recorded
- Filter definitions

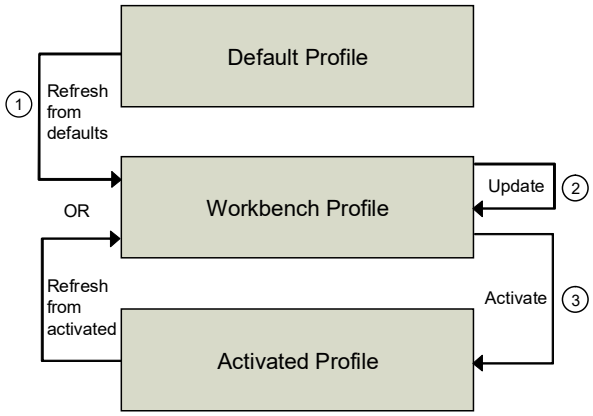
The life cycle of a profile consists of three phases:

- **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 293.

  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 electronic signature processing. See “Update Signature Profiles” on page 295.
- **The activated profile.** This is the profile used by the system to control electronic signature processing. It is copied from the workbench profile during activation along with a begin date, and it stays in effect until the begin date of another active profile for the same category. See “Activate Electronic Signature Profiles” on page 299.

Figure 11.4 summarizes the relationships between the three category profile types.

Fig. 11.4
Profile Flow



Setting up and using electronic signature profiles include these steps:

- Create electronic signature groups.
- Refresh workbench profiles.
- Update workbench profiles.
- Activate profiles.

Define Electronic 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 electronic signature functions use to manage the information retention and reporting process. This information affects electronic signature functions only after the profile is activated.

A category profile:

- Indicates whether signature functions are enabled for the category in general and for specific menu programs.
- Specifies control information that determines how electronic signature data displays when an enabled program runs.
- Maintains a list of tables and fields that defines the data to be signed. This data is included in signature records.
- Defines filters that can be used to determine whether electronic signature requirements apply to all records or only those containing specified values.

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 288. 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 electronic signatures, or to group related categories for signature purposes. Signature groups streamline the setup process by letting you refresh and activate the profiles for all member categories at once, instead of one profile at a time.

Example You might create a group called Control that includes the Inventory Control (0001) and Compliance Control (0004) categories so that you can refresh and activate both control program-related profiles at the same time.

Specify a group name, up to eight characters. An electronic signature group cannot have the same name as a category code.

Next, provide a brief description and choose 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 electronic signature functions, workbench category profiles are empty and must be manually populated. Use E-Signature Workbench Refresh (36.12.14.4) to update the empty profiles with the QAD-provided default information. You can refresh one category at a time or, optionally, refresh the profiles for an entire group of categories.

You can use this program later to restore the QAD-provided default data, modified in E-Signature Workbench Profile Maintenance, or to update workbench profiles based on existing active profiles.

Note Any changes you make with this program do not affect activated profiles currently in use.

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 electronic signatures for the specified profiles. When this field is Yes, an additional frame displays.

Refresh Profile Frame

If Refresh Profiles is Yes, the Refresh Profile frame displays.

Source Profile. Enter Activated or Default to indicate which profiles to use as the source for refreshing the profiles selected previously.

Activated: Each specified workbench profile is refreshed using the activated profiles in use on the date specified in Effective Date. The corresponding profiles must be in use on the date specified; otherwise, the system displays an error for each activated profile not found and the refresh does not occur for that profile.

Default: Each specified workbench profile is refreshed using the QAD-provided values. Select this value when initially setting up electronic signature functions to load the QAD-provided values into the profiles for the categories in which you plan to use signatures.

Effective Date. Enter a date when the activated source profile was in use. The workbench profile is refreshed using the active source profile settings in use on this date. If an activated profile was not in use on the specified date, an error displays and the target profile is not refreshed.

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 electronic signature functions for the profiles being refreshed.

If Refresh Profiles is No, the value specified here replaces the E-Signature On value in the current workbench profiles for the specified group or category. However, no other workbench data is updated.

When you refresh based on QAD-provided profiles, signature functions are turned on by default. You can use this field to override that setting.

Use E-Signature Workbench Profile Maintenance to change this value for individual profiles.

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 electronic signature processing works for each category
- Specifying the menu programs from the available list where signatures will be applied to the category
- Updating the list of tables and fields that are to be signed and included in signature records
- Setting up filters to control whether specific data is subject to or exempt from signature requirements

To disable electronic signatures for a profile that currently requires them, you must create a new activated profile for the category. Do this by updating the workbench profile and setting the E-Signature On value to No; then activate that new profile with the proper begin date. See “Activate Electronic Signature Profiles” on page 299.

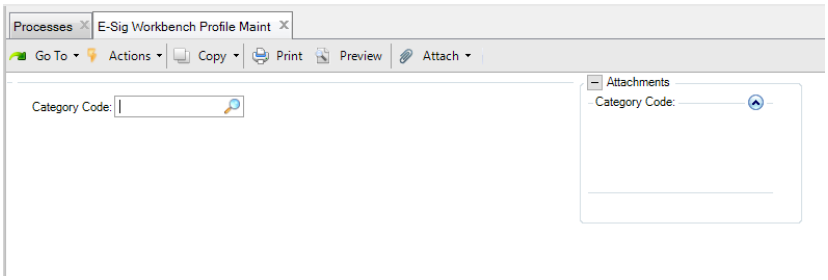
Use E-Signature Workbench Profile Report (36.12.14.6) to display the information updated in this program.

Note Some special considerations apply when you are setting up profiles that involve category 0007, Transaction History. See page 287 for information.

Specifying Control Settings

Figure 11.5 illustrates the first frame of E-Signature Workbench Profile Maintenance.

Fig. 11.5
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 electronic 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 electronic signature could contain many records of this type—so the mph_hist identification is not unique. However, all mph_hist records from the electronic signature instance are related to a single wr_route record, which serves as a unique identifier for the signed data. See “Tables and Fields” on page 288.

E-Signature On. Indicate whether the system should apply the electronic signature functions for the category defined in this profile when it is activated.

No: Electronic signatures do not apply to this category. Use this option to turn electronic signatures off for programs that currently require them. For example, if signatures are currently used and a new profile for this category with E-Signature On set to No is activated, electronic signature functions stop on the new profile's begin date.

Yes: Once this profile is activated, electronic signatures are required for this category as defined by the menu details and applicable filters.

When you refresh from QAD-provided default data, the value is Yes.

Display Latest E-Sig. Indicate whether the system displays the latest electronic signature when programs controlled by this profile are executed. See "Record Electronic Signatures" on page 300.

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 electronic signatures are used with these programs and the final data to be signed—including the transaction data—must be displayed to the user while prompting for the signature, records remain locked until the user successfully completes the signature. This record-locking during signing is necessary because all changes must be rolled back if the signature is not accepted. During this time, no other users can update these same locked records. This issue becomes even more problematic, for example, if the user decides to 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 electronic signature without scrolling through the data to be signed. In this case, they can still view all the fields by setting Scroll Details to Yes in the signature frame.

When the field is No, focus is on the frame that displays the data to be signed. To enter the signature, users must first choose End to exit that frame.

When you refresh from QAD-provided default data, the value is Yes.

Prompt for Remarks. Indicate whether the user can add an optional remark while entering electronic signature data. When this field is Yes, a 64-character updateable Remarks field displays in the signature frame. Remarks are included in the electronic signature record.

When you refresh from QAD-provided default data, the value is Yes.

Filter Mode. Specify the type of filtering the system will use in determining whether specific data requires electronic signatures. See “Filters” on page 289.

None: Filters are not used. The Filters and Filter Criteria frames do not display.

Inclusion: Only data meeting the specified filter criteria requires electronic signatures.

Exclusion: All data except those meeting the specified filter criteria require electronic signatures.

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 11.5 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 11.5
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 electronic 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 308. 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 clear 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 288.

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 electronic signature processing occurs for data associated with specified values. See “Filters” on page 289.

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 electronic signature processing, depending on the filter mode.

You cannot enter data ranges for a filter. Instead, enter multiple criteria values. Each criteria value displays on a separate line in the Filter Criteria frame.

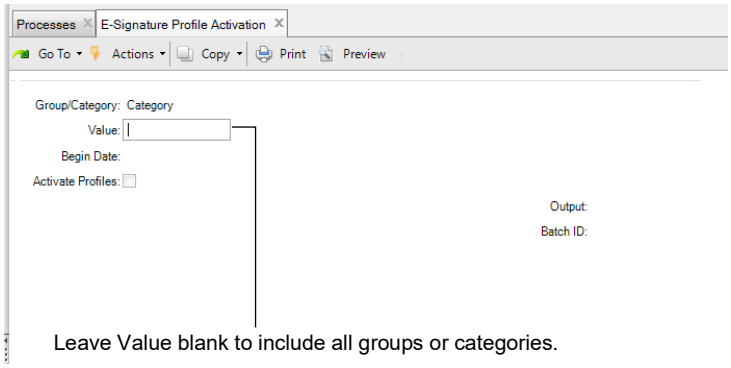
To filter on a blank value, enter the filter field name and leave Value blank. The system prompts you to confirm. A blank value is not a wildcard; instead, it only matches data where the value is actually blank.

Important Since the system does not validate this value, you should be careful when you set up filters. For example, if you are setting up an inclusion filter to require electronic signatures only for a single site and accidentally enter an invalid site code, the program will never prompt for a signature.

Activate Electronic Signature Profiles

After completing the workbench profiles, use E-Signature Profile Activation (36.12.14.8) to activate profiles for one category or a group of categories. Activated profiles are staged for electronic signature functions to begin on a future date; signature settings are not in effect immediately after a profile is activated.

Fig. 11.6
E-Signature Profile Activation (36.12.14.8)



Profiles cannot be activated on the begin date. Plan all changes ahead of time and activate updated profiles before their begin date. Profiles must have the begin date set to sometime in the future. Activated profiles become effective at 12:00 AM on the 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 288.

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 email message to system users who are assigned to the administrator role in Security Control (36.3.24). See “Email Notifications” on page 303.

Record Electronic Signatures

When profiles with E-Signature On set to Yes have been activated using E-Signature Profile Activation and the specified begin date is reached, the system automatically begins prompting for electronic signatures based on rules defined in the active profile.

When Display Latest E-Sig is Yes in the active profile, before displaying 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 287.

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 electronic 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 288.

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 electronic signature.

Note The points at which a program saves updates to the database may change when electronic signatures are enabled. See “Transaction Scoping” on page 302.

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 296. 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 284.

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 electronic signatures to the appropriate data, transaction scoping—the points during program execution when data is committed to the database—has been modified in some maintenance and transaction programs that can be signature enabled. See “Apply Profile to Menu Programs” on page 298.

For example, before electronic signature functionality was added, each frame in Inventory Control (3.24) was included in an individual transaction block. You could update the first frame, choose 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 electronic 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 electronic 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 electronic signature for each PCO to be incorporated or implemented.

Each PCO is processed in one transaction. If an error occurs during incorporation or implementation processing, all data related to this PCO is rolled back—including updates to product structures, routings, and so on. Other PCOs processed in the same program session are not affected.

If the user presses End in the E-Signature frame, the system does not create an electronic signature, and rolls back the incorporation or implementation transaction for the PCO. It then continues to process the next PCO.

Note You cannot use batch processing with Incorporation or Implementation when electronic signatures are enabled for the program. The Batch ID field does not display.

Email Notifications

The system generates and sends emails 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 electronic signature attempts exceeds the Maximum Access Failures value in Security Control.

For more information see "Define Security Control Settings" on page 284.

The email 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 electronic signature-specific messages have a comment type of ES. The comment reference varies depending on the specific purpose. The e-mail is constructed by starting with a specific comment, followed by one or more 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 email, contact the QAD system administrator. Do not reply to this email.
```

Signature Profile Activation Email

Comment Reference: email_esig_profile_activation

Comment Type: ES

The email sent for signature profile activation is similar to this example.

```
The purpose of this email is to inform you that one or more e-signature categories has
been activated. You have been included in this email 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 email, contact the QAD system administrator. Do not reply to this email.
```

Signature Failure Email

Comment Reference: email_failed_esig_prefix

Comment Type: ES

The email 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 email 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 email 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 electronic signatures are available in three areas:

- Setup
- Electronic signature reports
- Functional reporting for programs that are signature enabled

Setup Reports

The E-Signature Setup Menu has four reports that provide information on signature setup records:

- Use E-Sig Category Master Report (36.12.14.11) to view the top-table name and the filters available for categories.
- Use E-Signature Group Report (36.12.14.2) to view the categories assigned to each group.
- Use E-Sig Workbench Profile Report (36.12.14.6) to view the following kinds of information about the current workbench structure for a specified electronic signature category:
  - Settings that control processing and display of signatures in enabled programs
  - The list of programs that are signature enabled for the category
  - The list of field and tables that are included in the signature record
  - Optionally, information about filters associated with the category, if applicable

  Note Depending on whether you have updated or refreshed a workbench profile since last activating it, this report does not necessarily show the settings currently in use for a category. Use Activated E-Sig Profile Report to view that information.
- Use Activated E-Sig Profile Report (36.12.14.9) to view information about profiles that have been activated using E-Signature Profile Activation. It displays the same types of information as E-Sig Workbench Profile Report, but lets you specify a range of categories over a range of effective dates.

  Example To view all the profiles currently in use, leave the category code range blank and enter today's date in both date fields.

  Note Although a date range is not required in the selection criteria, consider entering one. This significantly reduces the time required to generate the report.

Electronic Signature Records for Quality Control

Electronic 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 electronic 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 electronic 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.

Electronic Signature Reports

The Enhanced Controls Menu includes three reports that let you:

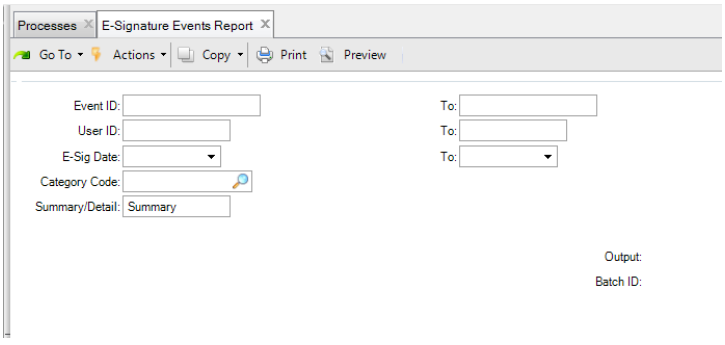
- Display signature events based on information related to the signature itself, such as the user, date, and meaning.
- Select database records based on ranges of values for fields in category top tables, and generate a report on related electronic signature history.
- Monitor sign-in history records for failed electronic 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.

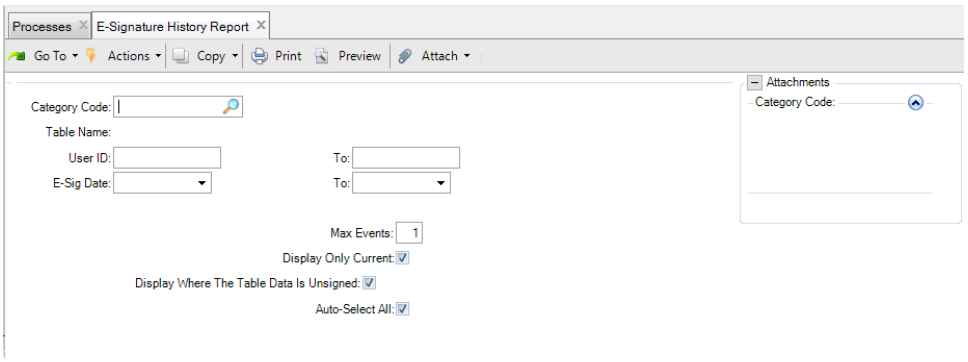
Fig. 11.7
E-Signature Events Report (36.12.4)



View Signature History

Use E-Signature History Report (36.12.5) to select database records and view historical electronic signature data associated with them. For example, you can report on the two latest signature events associated with a specified work order.

Fig. 11.8
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 electronic signature events to be included in the report for each selected record. The default is 1, which displays the latest signature event for each record that matches the data ranges in the E-Record Selection Criteria frame. If you enter a larger number, the system displays the latest first, then works backward through the number of events specified.

Display Only Current. Indicate whether the system should limit the selection to records in which no data has been updated since the latest electronic signature was recorded.

Display Where the Table Data Is Unsigned. Indicate whether the system should include records matching the criteria data ranges even if they are not covered by an electronic signature instance. When this is Yes, the output identifies records that do not have associated signatures.

Auto-Select All. Indicate if you want all the fields in the top table to be included in the report by default. You can modify the setting for individual fields as needed in the Report Display Fields frame. The default is Yes.

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 289.

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 electronic signature data in the output. When Display E-Signature Details is Yes, the system displays information about the signature such as the individual who signed the record, as well as values of the signed data fields.

Note The display of this field is conditional. It only appears on the user interface when both the following are true in the active profile for the appropriate category:

- E-Signature On is set to Yes. See page 294.
- The menu program has Apply selected. See page 298.

Based on those values, the reports and inquiries listed in Table 11.6 can include the Display E-Signature Details field.

Table 11.6
Reports and Inquiries Displaying Electronic Signature Data

Program	Menu	Category
PCR/PCO Detail Inquiry	1.9.2.8	0010
Print PCR/PCO	1.9.9.1	0009
Lot Master Inquiry	1.22.2	0005
Inventory Detail by Lot Inquiry	3.1.13	0006
Inventory Detail by Item 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, electronic signature data is not included regardless of this setting. Change the output device to view that data. This limitation does not apply to reports.

Archive and Restore Records

Use E-Signature Archive/Delete (36.12.14.22) to archive electronic 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 electronic signature creation date you want the system to consider. The system selects all records up to that date that have not previously been archived. 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 electronic signature records.

Chapter 12

Electronic Signatures in Adaptive UX

This section discusses how to set up and use electronic signatures functionality in Adaptive UX.

Overview ***312***
Explains the purpose of the electronic signature features, describes the planning steps when implementing electronic signatures, and explains the electronic signature workflow.

Set Up Electronic Signature Functionality ***313***
Explains the steps necessary to set up records that control when electronic signatures are recorded.

E-Signature History ***320***
Describes how to view records of the changes to data that required an electronic signature.

Record Electronic Signatures ***322***
Describes how electronic signatures are processed through the system with details on transaction scoping and product change control.

E-Signature Modes ***322***
Describes the principles of using E-Signature UI and API Modes.

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 was historically associated with a hard-copy signature on paper, it has been extended in many areas to electronic records. For example, the United States Food and Drug Administration (FDA), in 21 CFR Part 11, describes how electronic signatures can be used to support automated processing.

The electronic signature features of Adaptive UX support this requirement. You can configure your system to require users of certain fields or approval processes to enter a 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 Roles, Role Menus, and User Access to assign access to signature-controlled functions based on user roles. See “Role Menus” on page 129.

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.

Important Electronic signatures can be enabled in Adaptive ERP and Adaptive UX, and operate in both user interfaces simultaneously. However, you must set up and configure the functionality in both UIs separately. In addition, as you enable electronic signature configurations in Adaptive UX, you should disable the related functionality in Adaptive ERP by removing permissions to menu options. This ensures reports and histories for electronic signature events are confined to one interface with a consistent reporting structure. Contact QAD Support for assistance with Adaptive UX electronic signature configuration.

Note The E-signature functionality supports LDAP. The support of SAML will be implemented in the nearest releases.

Electronic Signature Planning Steps

Before electronic signature processing can begin, prerequisite planning steps must be completed.

The first activity in setting up electronic 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 Adaptive Applications fits into your overall business processes, as well as which specific electronic signatures support those processes.

- Determine security requirements for signed records; for example, assign appropriate role-based security to prevent users who should not sign records from accessing the fields that require signatures.

Electronic 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.

Electronic Signature Workflow

1. **Set up electronic signature reason codes.** Electronic 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 electronic signatures must have an “ESIG” reason type. See “Set Up Electronic Signature Reason Codes” on page 314.
2. **Define electronic signature control settings.** Define the settings in Security Control that determine how sign-in security is defined in terms of password structure and use rules. See “Define Security Control Settings” on page 314.
3. **Set up electronic signature configurations.** Use E-Signature Setup to define the fields and/or approval flows that require a user to provide an electronic signature. See “Define Electronic Signature Configurations” on page 315.
4. **Review electronic signatures using E-Signature History.** Use E-Signature History to review changes made to electronic signature-enabled fields. See “E-Signature History” on page 320.

Set Up Electronic Signature Functionality

When setting up electronic signature functionality, the following tasks must be completed:

- Set Up Electronic Signature Reason Codes
- Define Security Control Settings
- Define Electronic Signature Configurations

In addition, you should review your company’s web browser security policy. If a policy is not in place and enforced, your browser might offer to autofill credentials in forms that contain password fields, including the E-Signature window in which users record their electronic signature. Edit your browser settings and ensure the related security policies on managed computers are enforced to disable autofill of credentials.

Set Up Electronic Signature Reason Codes

The signature reason code is a critical element of the electronic signature. In regulatory environments, the signature record typically must include the meaning of the signature. The system uses reason codes to provide the meaning.

Each time the system prompts for an electronic signature, the user must provide a valid reason code. For example, reason codes might indicate that a quality record has been approved, reviewed, or inspected. See “Record Electronic Signatures” on page 322.

Use Reason Codes to define signature reason codes that are appropriate to your environment.

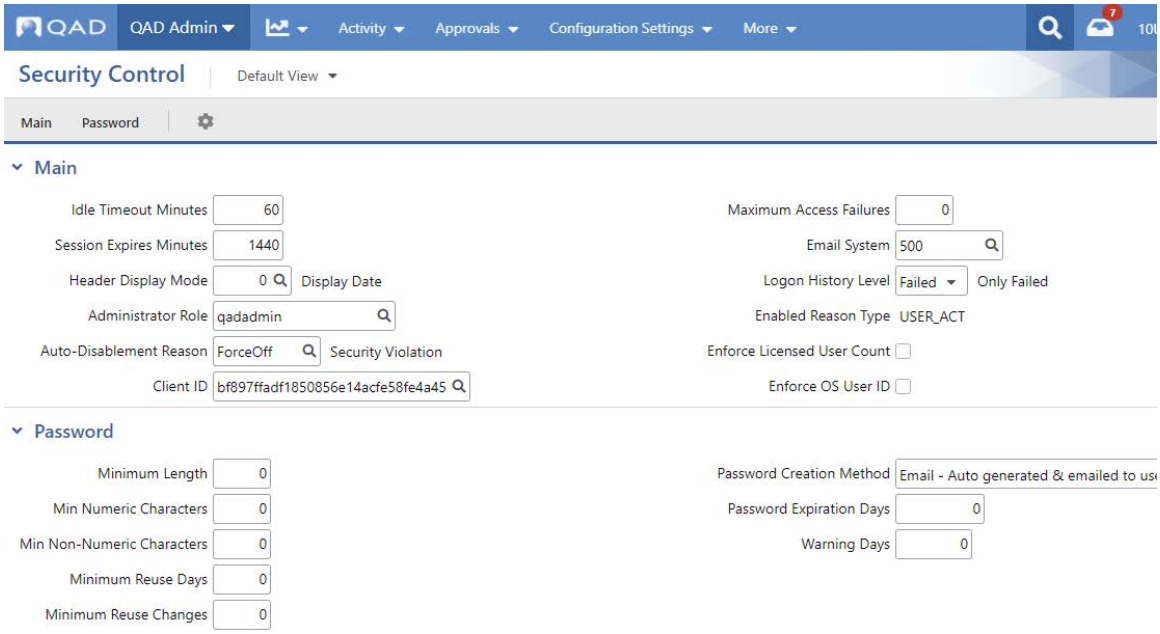
Important All reason codes used by electronic signatures must be associated with the QAD-provided ESIG reason type. Reasons of any other type cannot be entered in the signature prompt frame.

Define Security Control Settings

To prevent unauthorized individuals from applying electronic signatures using another user’s ID, electronic 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 electronic signature functionality, define the security control settings in Security Control to see how sign-in security is defined in terms of password structure and user rules.

Fig. 12.1
Security Control



Two fields directly control how the system manages unsuccessful electronic 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 Roles—assigned to the system users who are notified by email when a session is terminated because of excessive unsuccessful signature attempts.

Define Electronic Signature Configurations

You can configure the electronic signature functionality for any field or approval flow in your system.

Note If you plan to restrict who can sign individual fields, you must enable field-level security on the business components that contain the electronic signature fields. See "Securing Fields and Field Groups from Within Adaptive UX" on page 152 for details.

Electronic Signature Default Configurations

QAD provides a number of pre-set configurations that are available on the E-Signature Setup screen. You can enable these configurations by selecting the Active checkbox in each record.

Table 12.1
Default Electronic Signature Configurations

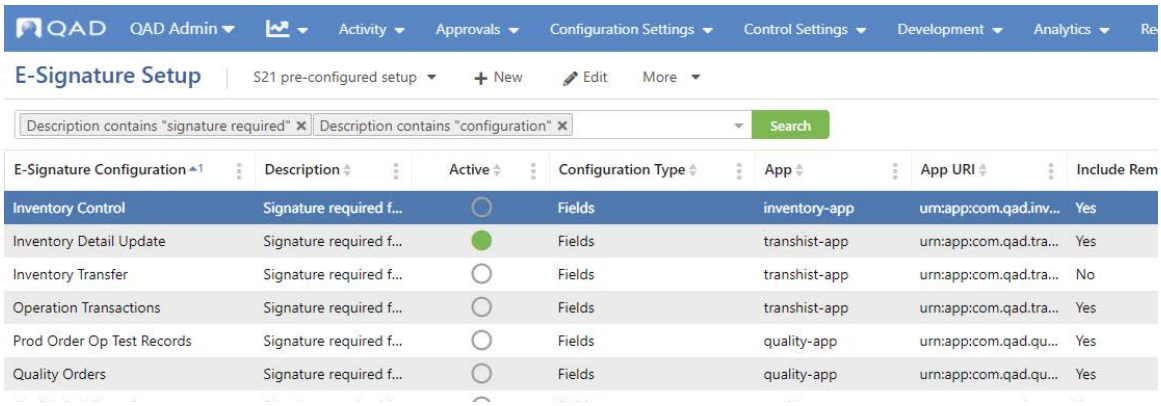
Configuration Name	Change Requiring a Signature
Asset Work Order Close	An asset work order is closed
Inventory Control	Changes are made in the Compliance panel to any of the following: • Compliance Active • Modify Component Issue • Modify Co/By Product Receipts • Lot Control Level • Single Lot per Purchase Order Receipt • Single Lot per Work Order Receipt • Single Lot per Repetitive Receipt Changes are made in the Inventory panel to any of the following: • Default Site • Tolerance From • Class A (both fields) • Class B (both fields) • Class C (both fields) • All Others (both fields) • Picking Order • Picking Sequence • Issue Days
Inventory Detail Update	Changes are made to Expire Date, Grade, Assay %, or Inventory Status Tracks transaction history for certain transaction types that occur only on certain transactions

Configuration Name	Change Requiring a Signature
Inventory Transfer	Materials are transferred to new locations, including bulk transfers ***Note***: If your system is using serialization, you must enable the Serial History configuration when you activate Inventory Transfer.
Operation Transactions	Operation reporting transactions are performed on production operation reporting actions
Production Order Operation Test Records (Prod Order Op Test Records)	Changes are made to test status
Quality Orders	Order Status changes to Closed
Quality Test Records	Test status changes to Closed, Canceled, or Approval Pending
Serial History	Changes are made to any of the following: • Transaction Number • Serial ID • Transaction Type ***Note***: Enable the Inventory Transfer configuration when activating the Serial History configuration. The Serial History is required when serialization is in use.
Test Specification	Test Revision Status changes to Released or Obsoleted

E-Signature Setup Screen

Use the E-Signature Setup screen to define and manage electronic signature configurations that are triggered by changes to individual fields or that are part of an approval process flow.

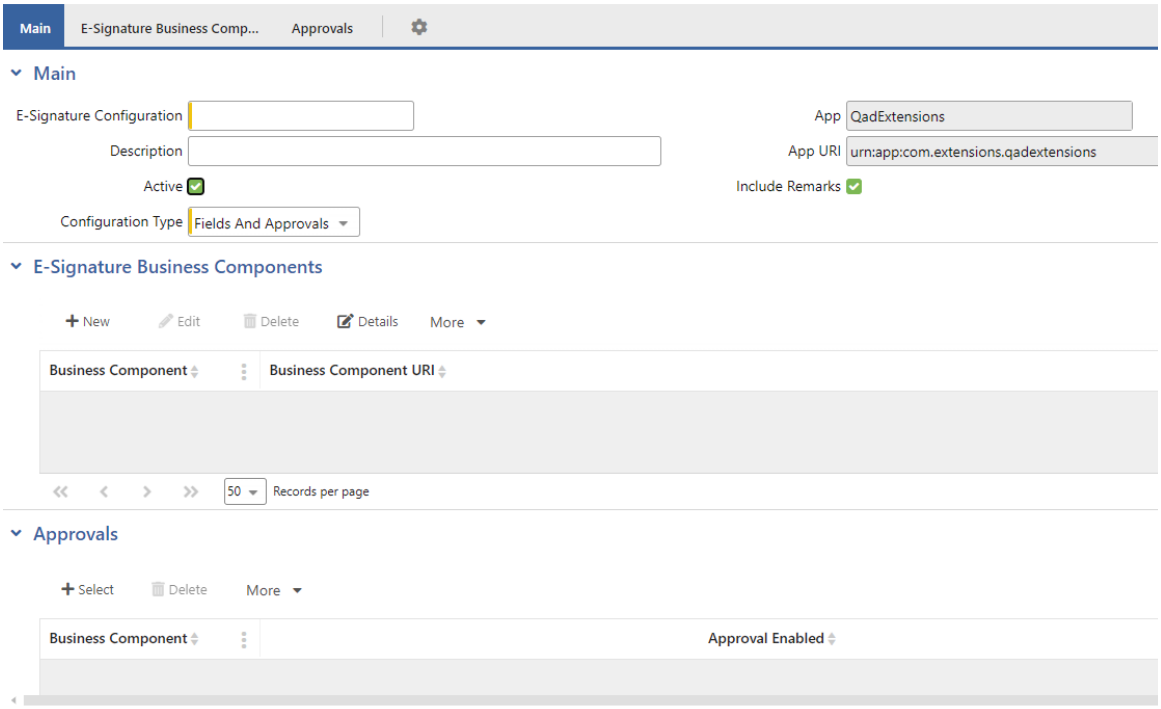
Fig. 12.2
E-Signature Setup



The E-Signature Setup screen lists the existing electronic signature configurations. Configurations that are active in the system have a green circle in the Active column. Configurations that are not active have a gray outline of a circle in the Active column.

Click New to create a new configuration.

Fig. 12.3
New Electronic Signature Configuration



Define the following fields for the new configuration.

Main

E-Signature Configuration. Enter a name for the new electronic signature configuration.

Description. Enter a brief description of the electronic signature configuration. This description can provide more context for anyone accessing the E-Signature Setup screen. The field can be up to 70 characters long.

Active. Select this checkbox to make the electronic signature configuration active upon successful save.

Configuration Type. Select one of the following from the drop-down menu:

- Fields. Select Fields to require an electronic signature for fields you designate as part of the configuration process.
- Approvals. Select Approvals to require an electronic signature for an existing approval configuration.
- Fields and Approvals. Select Fields and Approvals to require an electronic signature for both specific fields and an existing approval configuration.

App. Displays the app in which this electronic signature configuration is located.

App URI. Displays the URI of the app in which this electronic signature configuration is located.

Include Remarks. Select this checkbox to include a field for remarks on the E-Signature pop-up window when users record their signatures. This content appears in the E-Signature History screen's Remarks column.

E-Signature Business Components

The E-Signature Business Components option is visible if you selected Fields or Fields and Approvals in the Configuration Type drop-down menu. The grid lists the business components that have fields that prompt for electronic signatures. The business components require additional configuration to set the fields that require electronic signatures. To add a business component to this configuration, click New. To edit an existing entry, highlight the record and click Details.

Approvals

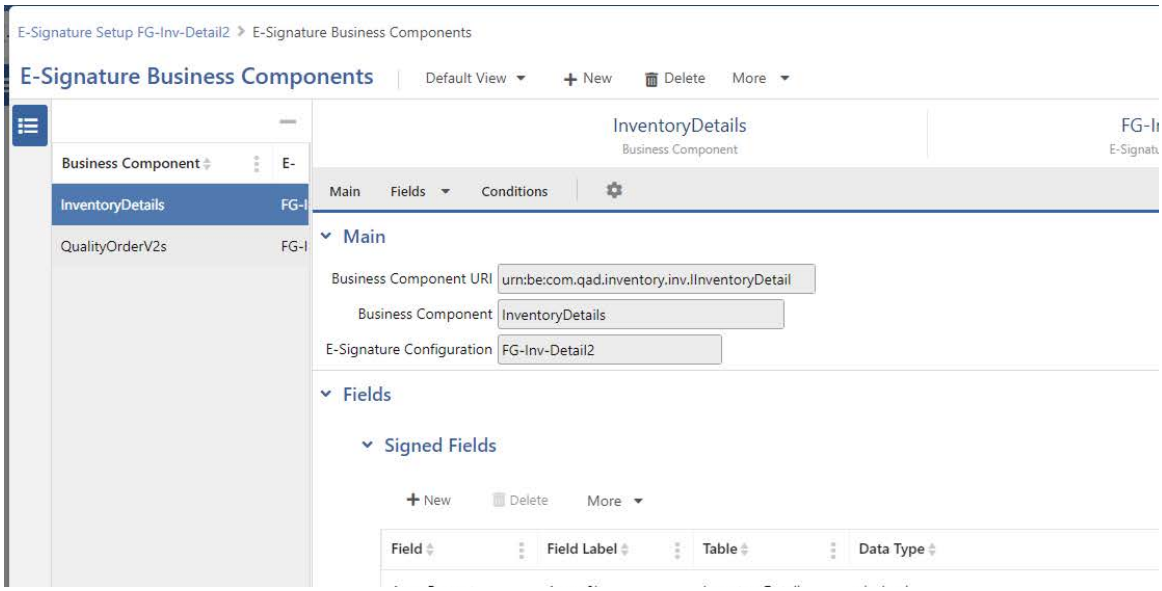
The Approvals option is visible if you selected Approvals or Fields and Approvals in the Configuration Type drop-down menu in E-Signature Setup.

To add a new approval process flow to the electronic signature configuration, click Select and then choose a business component from the Approval Configuration screen.

E-Signature Business Components Details

Use E-Signature Business Components to define the fields that require a user signature, as well as the referenced fields and conditions that make up the electronic signature configuration for one business component.

Fig. 12.4
E-Signature Business Components



Main

Business Component URI. Use the lookup to select the business component to add to the configuration.

Business Component. The business component's name defaults from the selected business component URI.

E-Signature Configuration. The electronic signature configuration defaults from the main record.

Fields

The Signed Fields and Reference Fields options are visible if you selected Fields, or Fields and Approvals in the Configuration Type drop-down menu in E-Signature Setup.

Signed Fields

The Signed Fields grid lists the fields in the business component that require a signature with any change. Click New to add a field to the configuration.

Note Do not enter fields you intend to make conditional. Use the Conditions panel for fields that require signatures only when a certain condition is met.

Field. Select a field from the lookup. The lookup is filtered to the fields in the selected business component.

Field Label. The field label associated with the selected field.

Table. The table in which the selected field is found.

Data Type. The data type of the selected field, such as decimal, date, or character.

Reference Fields

Reference fields are included as part of an electronic signature configuration to allow for more refined searching and filtering on the E-Signature History screen. They do not require an electronic signature when they are updated.

Reference fields are limited to five per business component.

Sequence. Set this free-form field to a value from 1 to 5. The number corresponds to the associated Reference Field column on the E-Signature History screen. Best practice is to have a consistent sequence assignment of reference fields across your system. For example, any business component that includes Item as a reference field should designate Item as Sequence setting 1 while Equipment Type should be set to Sequence setting 4. This ensures the Reference Field columns in E-Signature History can be used to the fullest extent of the system when searching and filtering.

Reference Field. Select a field from the lookup, which is filtered to the fields in the selected business component.

Field Label. The field label associated with the selected field.

Table. The table in which the selected field is found.

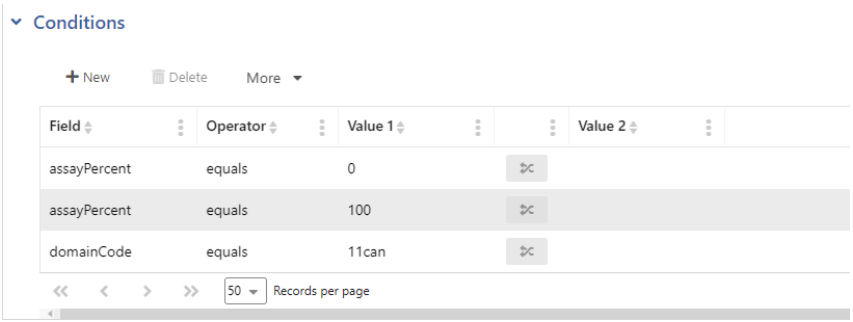
Data Type. The data type of the selected field, such as decimal, date, or character.

Note For non-previewable business components, the system does not track the changes in field values, and you are prompted for credentials at any field update. You cannot set up signing certain fields only. For more information about using previewable and non-previewable business components, see "E-Signature Modes" on page 322.

Conditions

Use the Conditions grid to limit the scope of the electronic signature configuration.

Fig. 12.5
Electronic Signature Conditions



Depending on the specific requirements of your environment, you may not need to record electronic signatures for all records of a given type. For example, you might want to require electronic signatures only on inventory transactions involving a specific site or when changes are made to pieces of equipment that are used in production.

Field. Select the field for the condition you are setting.

Operator. Select the appropriate operator.

Value 1. Enter an appropriate value for the selected field and operator.

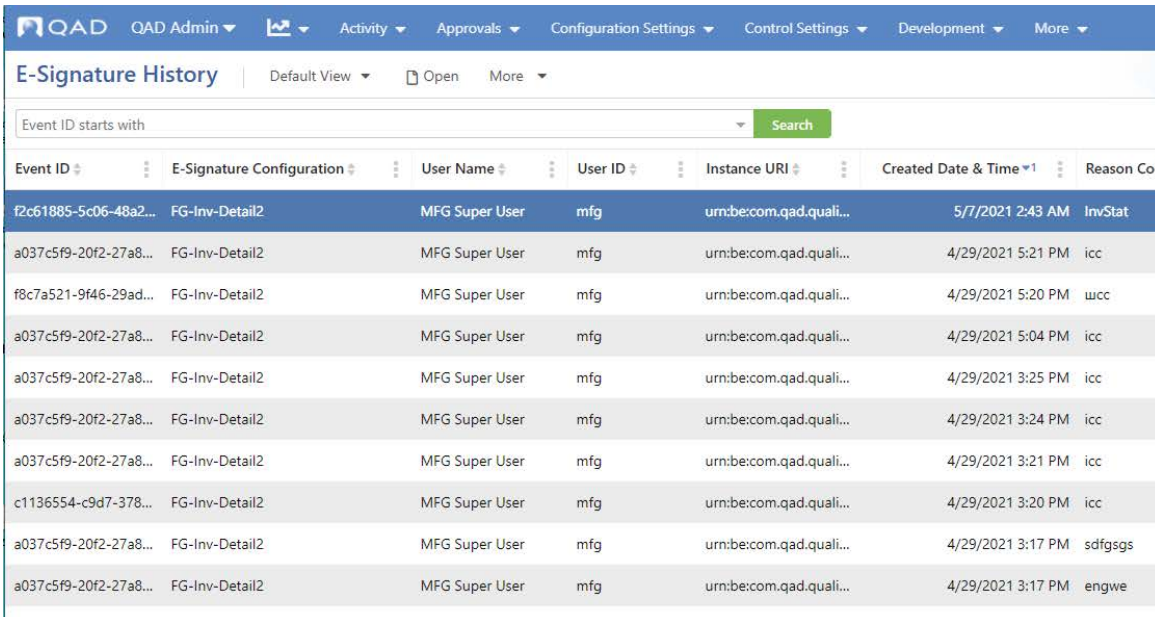
Value 2. If required, enter a second value.

Note You can also use conditions in e-signature API Mode. For more information about using e-signature in API Mode, see “E-Signature Modes” on page 322.

E-Signature History

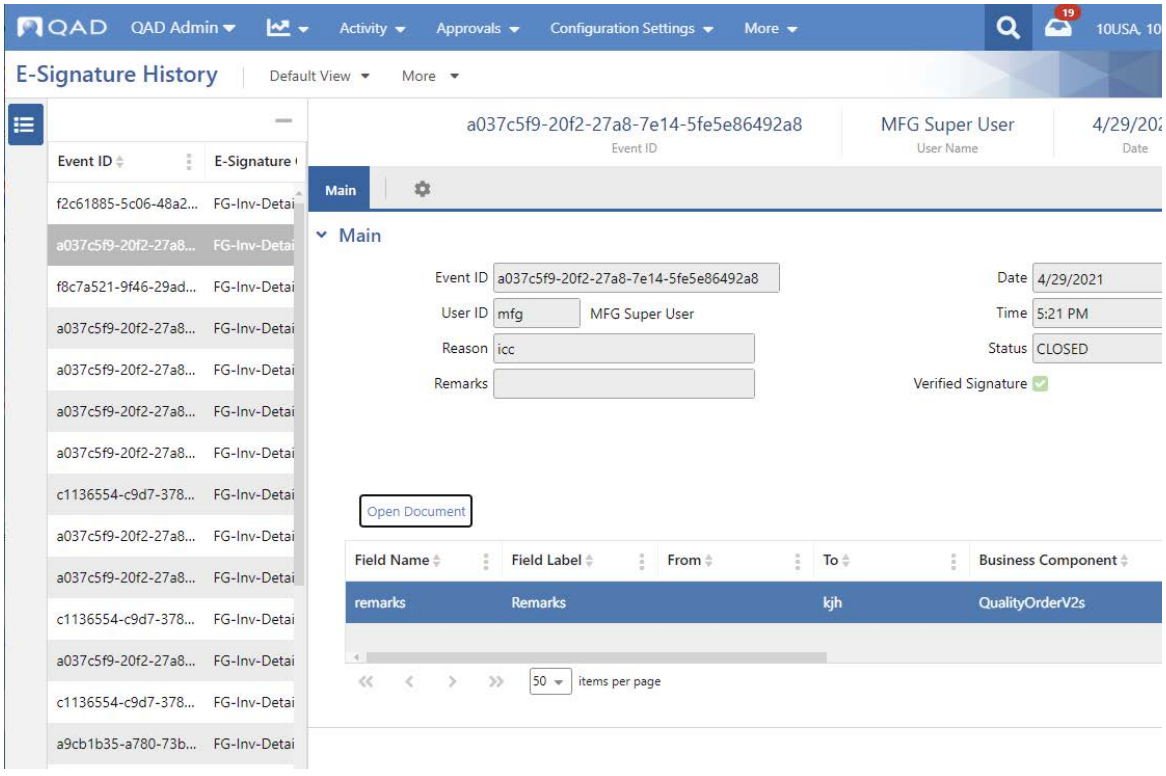
You can use E-Signature History to review changes made to electronic signature-enabled fields. Each historical record includes the field’s original content and its changed content, along with the user ID of the user who made the change, the time and date of the change, and the reason for the change.

Fig. 12.6
E-Signature History



To view the details of an event ID, double-click the record.

Fig. 12.7
E-Signature History Details

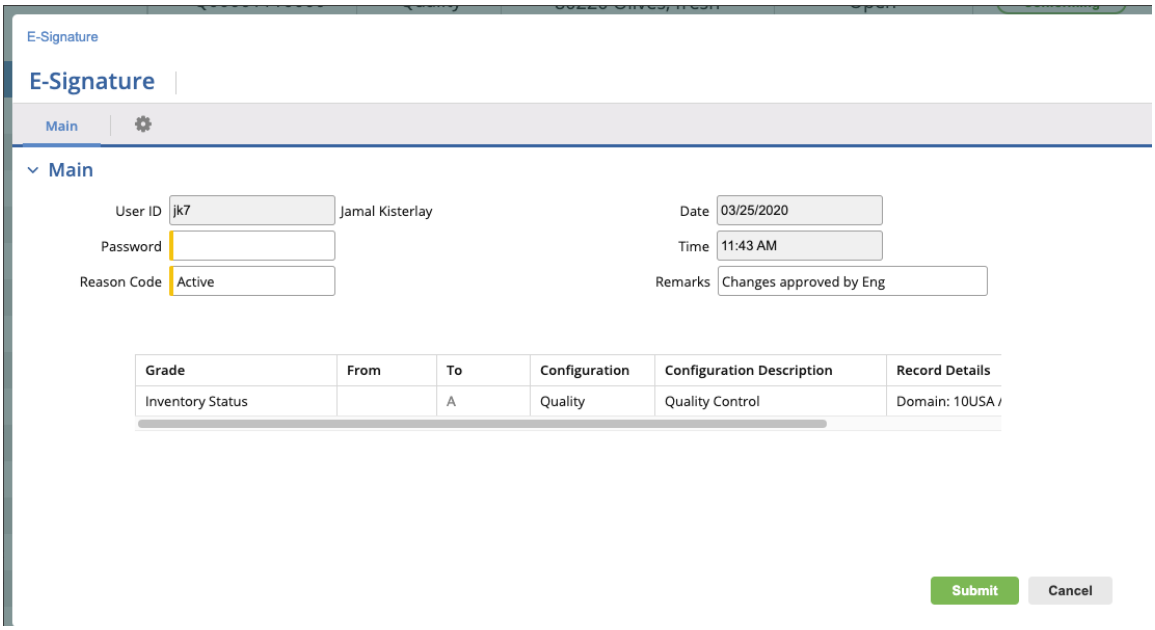


The individual record displays the data tied to this electronic signature event and links to the document that was changed. Click the Open Document link, highlighted in Figure 12.7, to open the record where the change was made.

Record Electronic Signatures

When the electronic signature configuration is complete and the Active checkbox is selected, the system automatically begins prompting for electronic signatures. No changes are made in the database until users successfully enter their passwords for fields or approvals requiring electronic signatures.

Fig. 12.8
E-Signature



The top area of a signature display includes three fields that cannot be updated: the user ID of the user who applied the signature, and the date and time of the event. Users must enter their password and the reason code. If Include Remarks was selected during the electronic signature configuration setup, users also can enter information about the change in the Remarks field.

The table in the lower area of the screen displays the data that is being changed and the information specific to the change. The From column is blank for fields that did not have a previous entry.

Note By design, some electronic signature configurations, such as Inventory Detail, do not include the lower table.

If a user enters an incorrect password, the system does not update the record.

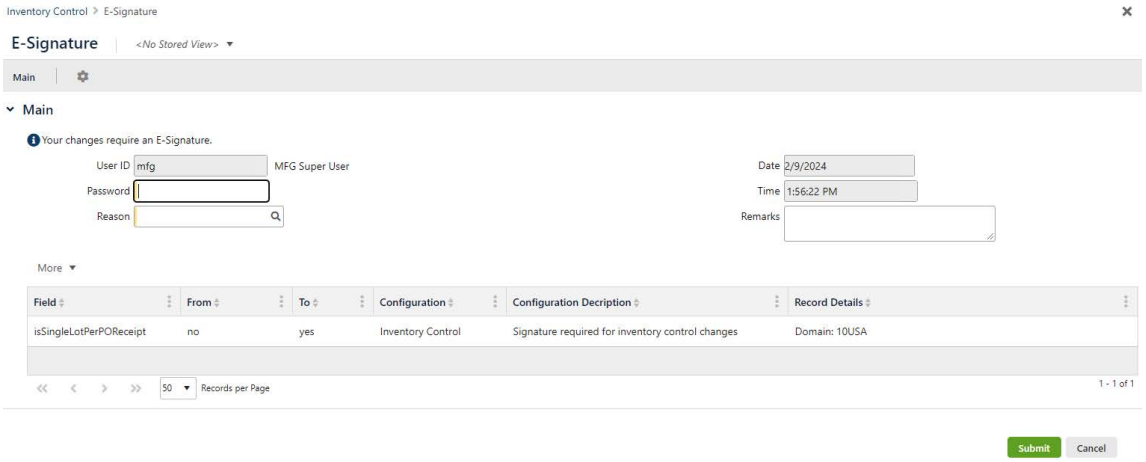
E-Signature Modes

In Adaptive UX, you can use the e-signature functionality for the following types of business components:

- Previewable
- Non-Previewable

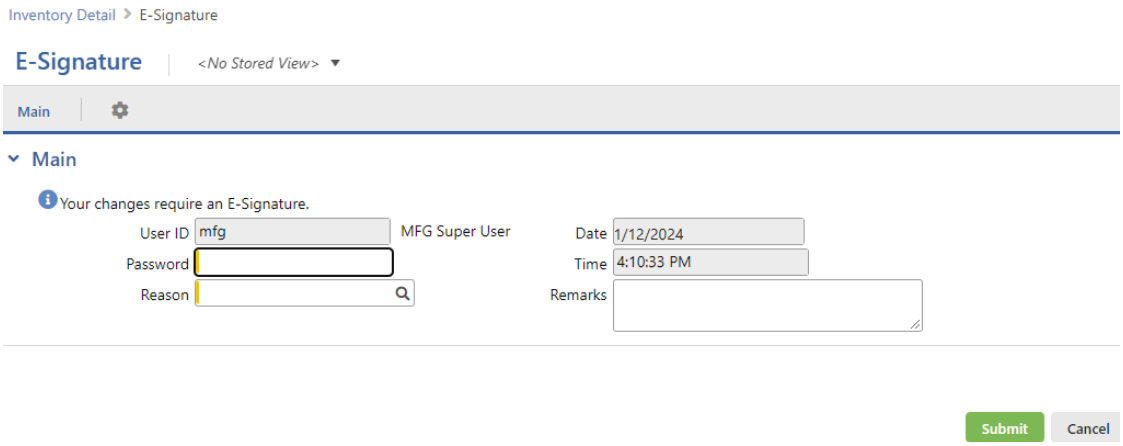
When signing changes in previewable business components, you can preview the field value changes in a separate e-signature pop-up before you sign and commit the transaction. The changed values are displayed in the From and To columns of the grid in a separate e-signature pop-up window, as shown in Figure 12.9.

Fig. 12.9
Inventory Control, E-Signature Pop-up



With non-previewable business components, you cannot see the field value changes during the signing operation. The grid with the From and To columns does not display in the e-signature pop-up, as shown in Figure 12.10.

Fig. 12.10
Inventory Detail, E-Signature Pop-up

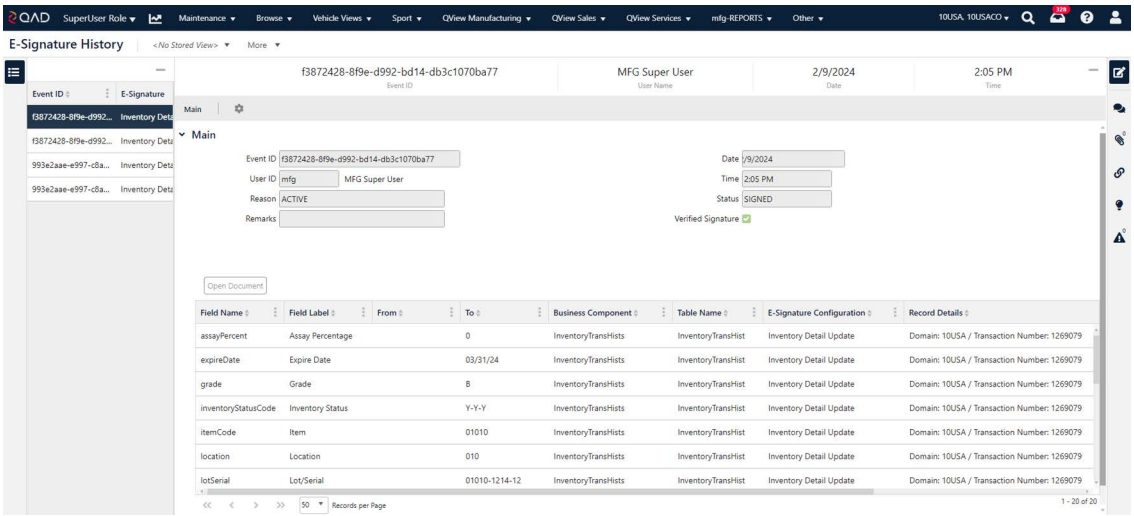


During an e-signature flow, the non-previewable business components use database sequences with the following technical limitation: sequence increments cannot be undone with a database transaction. This causes sequence gaps. Since you may not want to sign the changes and your operation may in fact be undone, the system does not display any preview grid with changed field values.

However, you can view the field value changes after signing them by using E-Signature History, as shown in Figure 12.11.

Note When you modify a record, the From and To fields are populated with previous and new values accordingly. However, when you create a new record, the From field remains blank.

Fig. 12.11
E-Signature History

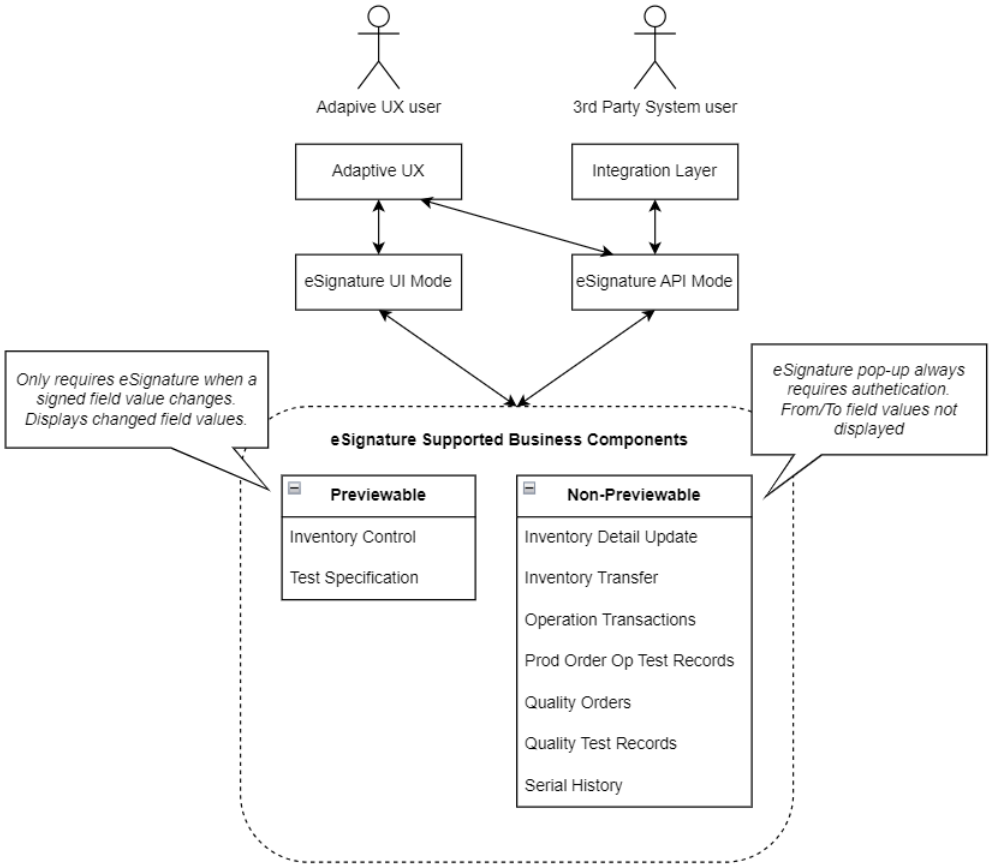


For both types of business components described above, you can use the following e-signature modes:

- E-Signature UI Mode
- E-Signature API Mode

Figure 12.12 shows the principle of user interaction with e-signature modes and different types of business components.

Fig. 12.12
User Interaction with E-Signature Modes and Business Components



E-Signature UI Mode

For e-signature UI mode, Adaptive UX provides user interface dialogs for signing operations. This mode is used by users who directly enter data in Adaptive UX.

E-Signature API Mode

For e-signature API Mode, Adaptive UX provides REST API endpoint to obtain an e-signature Token and pass it with the operation that requires an electronic signature. This mode is used by the integrated third-party systems to submit API requests that change data requiring e-signature.

API E-Signature Mechanism

You must receive an e-signature token when a business component with an active e-signature configuration takes part in an API request. In this case, you receive one of the `com.qad.qra.esig.ESignatureRequiredException` or `com.qad.qra.esig.APIModeRequiredException` errors, as shown in Figure 12.13 and Figure 12.14.

Fig. 12.13
Error for E-Signature with Field Value Changes Preview


```
{
    "submitResult": {
        "errors": [
            {
                "severity": 1,
                "code": "0",
                "message": <variable base64 encoded value>,
                "fieldName": "",
                "messageType": "com.qad.qra.esig.ESignatureRequiredException",
                "context": <variable base64 encoded value>,
                "fieldValue": "",
                "callStack": <variable correlation ID>,
                "cause": null,
                "gridId": null,
                "correlationId": null
            }
        ],
        "showResult": true,
        "resultMessage": "",
        "success": false,
        "errorSeverity": 1
    },
    "data": null
}
```


Fig. 12.14
Error for E-Signature without Field Value Changes Preview


```
{
    "submitResult": {
        "errors": [
            {
                "severity": 1,
                "code": "0",
                "message": "E-Signature API Mode is required.",
                "fieldName": "",
                "messageType": "com.qad.qra.esig.APIModeRequiredException",
                "context": "",
                "fieldValue": "",
                "callStack": <variable correlation ID>,
                "cause": null,
                "gridId": null,
                "correlationId": null
            }
        ],
        "showResult": true,
        "resultMessage": "",
        "success": false,
        "errorSeverity": 1
    },
    "data": null
}
```


To obtain an e-signature token and bypass the errors above, you must make a POST call to the `/api/qracore/esignature/token` REST API with the following payload:

Fig. 12.15
POST Call Payload

```
{
  "password": <Password string for the current user>,
  "reasonCode": <Reason Code string to be recorded with the eSignature event>,
  "remarks": <Remarks string to be recorded with the eSignature event>
}
```

The successful response will contain the e-signature token value, which is a base64 encoded string, as shown in Figure 12.16.

Fig. 12.16
E-Signature Token

```
{
    "submitResult": {
        "errors": [],
        "showResult": true,
        "resultMessage": "",
        "success": true,
        "errorSeverity": 0
    },
    "data": {
        "password": "",
        "reasonCode": "COMPLY",
        "remarks": "test",
        "token": "eyJhbGciIDogIkhTMjU2IiwidHlwIIA6ICJKV1QifQ.eyJleHAiOjE3MDY2OTc1OTEsImlhdCI6MTcwNjYxMzMzOSwiaXNzIjoidXJuOmNsaWVudGlkOm3iMTBmOTM3MzMxOTRhODFiYzE0NDQ1MTA4NGM0NzU5IiwiczVtIjoidXJuOnNlc3Npb25pZDpBOTcwNjJCC
    }
}
```


The received token must be attached to the `X-QAD-Esig-Token` HTTP request header.

Chapter 13

Auditing

This section discusses how to set up the auditing functionality in your system.

Overview ***330***
Defines auditing and explains how the Auditing module works.

Plan Auditing ***331***
Describes what to consider before performing an audit.

Set Up Auditing ***333***
Describes the requirements for configuring auditing for databases, importing policies, enabling auditing for specific areas, and generating audit reports.

Archive Database ***340***
Describes how to set up archive databases, connections, report on them, and customize archive/load scripts.

Generate Audit Trail Reports ***344***
Explains how to generate reports against application and archive databases.

Export Audit Policy ***351***
Explains how to export audit policies using Audit Policy Export.

Disable Auditing ***352***
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. 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 QAD does not recommend importing custom policies into the system nor using Progress tools to change QAD's default policy. Custom policies may cause conflicts on policy configuration.

Below is a list of menus and programs for the auditing module.

Table 13.1
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

Number	Menu Label	Program
36.12.13.2	Audit Policy Export	atplexp.p
36.12.13.5	Audit Configuration Maintenance	atplmt.p
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 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

Most application data reside in the qaddb (mfgdb) database, therefore it is common to audit-enable this database.

In addition, the qadadmin (qadadm) database houses the EDI tables and you may need to enable auditing for this second 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. The system prevents you from enabling such tables for auditing, whether they are standard or custom tables, and 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. 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. QAD recommends only audit-enabling tables needed to meet your auditing requirements, such as control tables or security configuration. For example, security and control tables may be audit-enabled to ensure important changes are logged in the audit data.

Before audit-enabling tables in a production database, QAD suggests validating the 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 separate 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, load the license for Enhanced Controls and do the tasks described in the following sections:

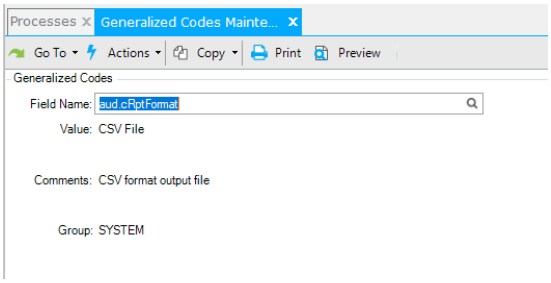
- “Create Generalized Codes to Enable CSV Output” on page 333
- “Enable Auditing for the Database” on page 333
- “Configure Database Options and Audit Permissions” on page 334
- “Import Audit Policy” on page 337
- “Enable Auditing on Selected Tables” on page 338
- “Enable Auditing on Selected Fields” on page 339

Create Generalized Codes to Enable CSV Output

The Audit Trail Report – App DB and the Audit Trail Report – Arc DB can be output in CSV format and imported into spreadsheet software. The necessary codes are automatically created in the system domain but you must manually create the codes in other domains. If you do not use CSV files, this step is not required.

1. Go to Generalized Codes Maintenance (36.2.13).

Fig. 13.1
Generalized Codes Maintenance



2. In Field Name, enter `aud.cRptFormat` or search for the field in the lookup. Select Next.
3. In the Value field, enter CSV File, then select Next.
4. The Comments and Group fields should automatically populate with:
   - CSV format output file
   - SYSTEM

   If they do not display these settings, enter them in the appropriate fields.
5. Select Next.

Enable Auditing for the Database

The database must be offline to enable auditing. In most cases, enable auditing on the database and archive database with these commands:

```
> yab -deactivateidx database-qaddb-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
```

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.

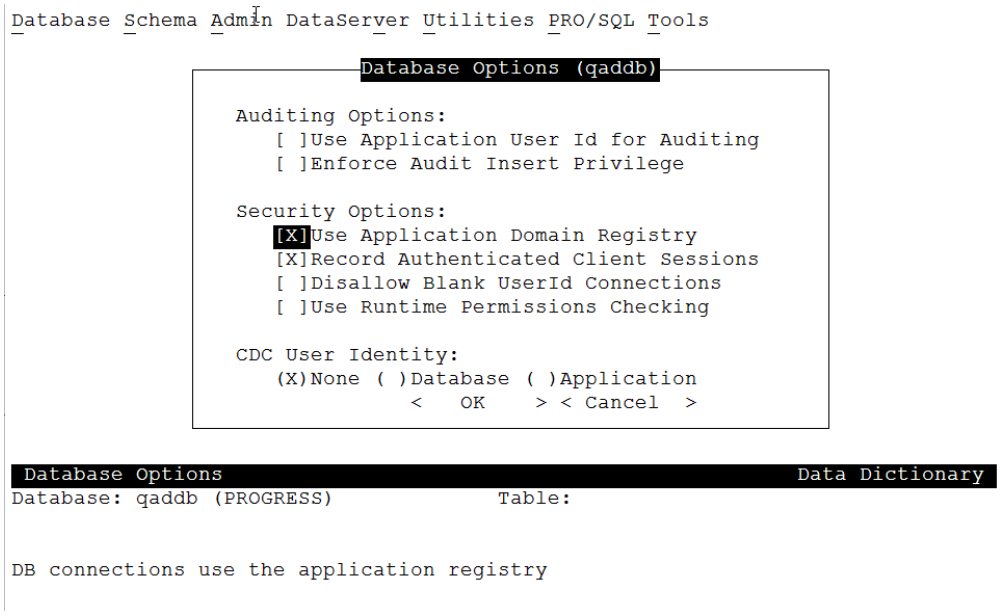
For each of the databases you have updated and enabled for auditing, you need to set up audit permissions. In addition, if you have converted from a non-YAB-managed environment that did not have auditing set up before bringing over your databases, you also must configure the database options.

Configure Database Options

Important This step is only required for systems that have been converted from a non-YAB-managed environment that also did not have auditing set up before the conversion. Continue to “Grant Audit Permissions” on page 335 if your databases are already configured.

Set up the new database options in Progress using the Data Administration menu. Choose Tools > Data Dictionary > Admin > Database Options ....

Fig. 13.2
Database Options Settings



Select the following options:

- Use Application Domain Registry
- Record Authenticated Client Sessions

Grant Audit Permissions

To access audit-related menus, a user must be granted specific audit permissions. Those permissions are:

- Audit Administrator — An authenticated user who has been granted privileges to create, update, and delete audit policies and read audit data.
- Application Audit Event Inserter — An authenticated user who has been granted privileges to generate application audit events. Note that in ABL applications, application of this privilege is optional and disabled by default; in SQL applications, application of the privilege is enabled by default and cannot be disabled.

  The application audit event inserter does not have privileges to archive audit data or policy tables.
- 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. Any user who is going to run an audit report must be set up with this permission.

Note The Audit Administrator is not an Audit Data Archiver nor Audit Data Reporter.

Table 13.2
Permission Required for Audit Menu Access

Program	Menu	Permission 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
Document Audit Trail Reports	36.12.12	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, configure the `db.INSTANCE.audit.auth.NAME` settings in the `configuration.properties` file.

Table 13.3
Audit Permissions

Setting	Description
db.INSTANCE.audit.auth.NAME	Used to assign audit permissions to users.
db.INSTANCE.audit.auth.NAME.users	A comma-delimited list of users.
db.INSTANCE.audit.auth.NAME.permissions	A comma-delimited list of audit permissions to assign to the users. The following values are accepted: • audit-administrator • application-audit-event-inserter • audit-data-archiver • audit-data-reporter

Replace INSTANCE with one of the databases you have updated and enabled for auditing. Replace NAME with a unique value you specify to differentiate pairs of settings for users and permissions, such as `admin` for administrative permissions, `archiver` for archive permissions, and `reporter` for those needing to run audit reports.

For example, the following settings grant Audit Administrator permission to two users, audit-admin1 and audit-admin2.

```
db.qaddb.audit.auth.admin.users=audit-admin1,audit-admin2
db.qaddb.audit.auth.admin.permissions=audit-administrator
```

This next example grants Audit Data Archiver permission to an archive user, named audit-archive1.

```
db.qaddb.audit.auth.archiver.users=audit-archive1
db.qaddb.audit.auth.archiver.permissions=audit-data-archiver
```

As previously noted, any user who is going to run an audit report must be set up with Audit Data Reporter permissions. For example:

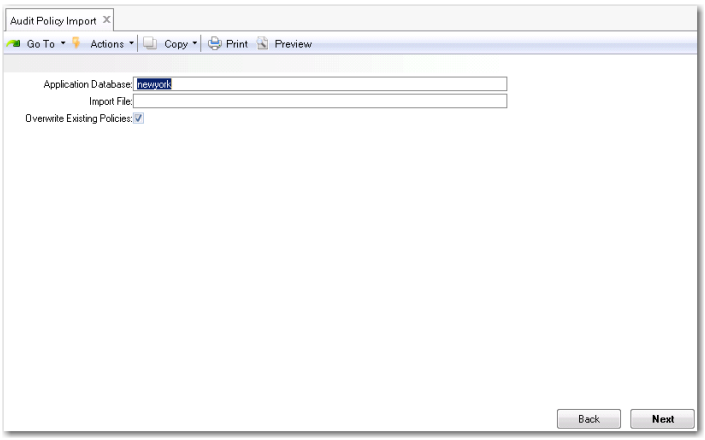
```
db.qaddb.audit.auth.reporter.users=audit-report1
db.qaddb.audit.auth.reporter.permissions=audit-data-reporter
```

Audit permissions are applied during an update or directly by running `database-INSTANCE-auditing-update`. When permissions are applied, YAB ensures that the permissions in the database match what is configured, revoking permissions that do not match the configuration. Some permissions like “Audit Data Reporter” are used within the application and may be granted to application users. If no permissions are configured, permissions must be manually set up using the Progress Data Dictionary. Refer to the Progress documentation for details.

Import Audit Policy

You can import audit policies from Progress policy XML files using Audit Policy Import (36.12.13.1).

Fig. 13.3
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.

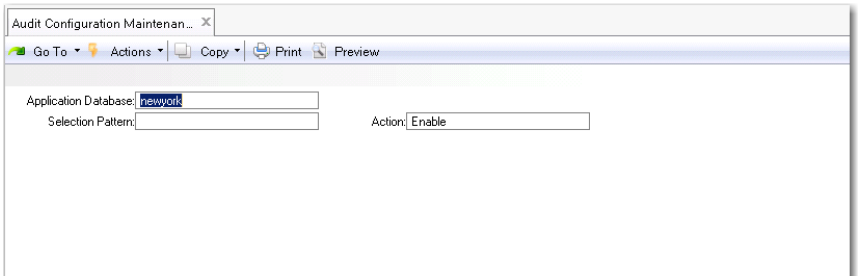
The default policy only covers tables whose identifying fields are different from primary keys. For most non-Financials tables, the primary keys can be used as identifying fields, so these tables do not appear in the default policy. For most Financials tables, however, the table has a primary key, which is a sequence identifier, and one or two unique indexes. One unique index is used for 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. 13.4
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*`.

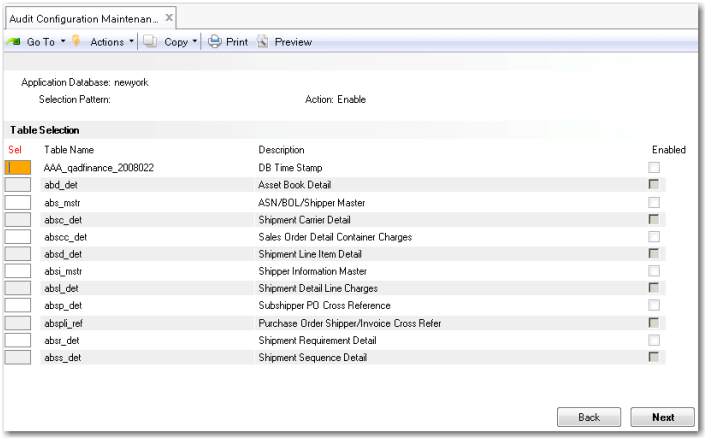
Action. Enter the code that represents the action you want to perform on selected tables:

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. 13.5
Audit Configuration Maintenance Table Selection



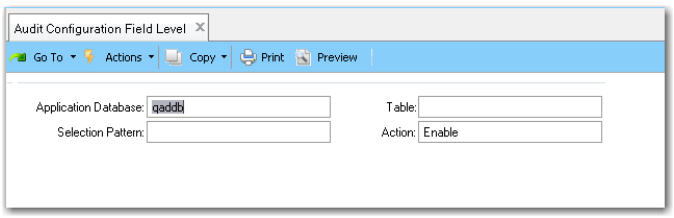
Use the up and down arrow keys to scroll through the list of tables. Use the space bar to select the tables whose Enabled settings you want to change. An asterisk symbol (*) displays at the front of the row of each table you select. To toggle the Enabled settings, select individual tables using the space 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 338.
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. 13.6
Audit Configuration Field Level



3. Use Audit Policy Export (36.12.13.2) to export all policies, including `qadmainpolicy`.

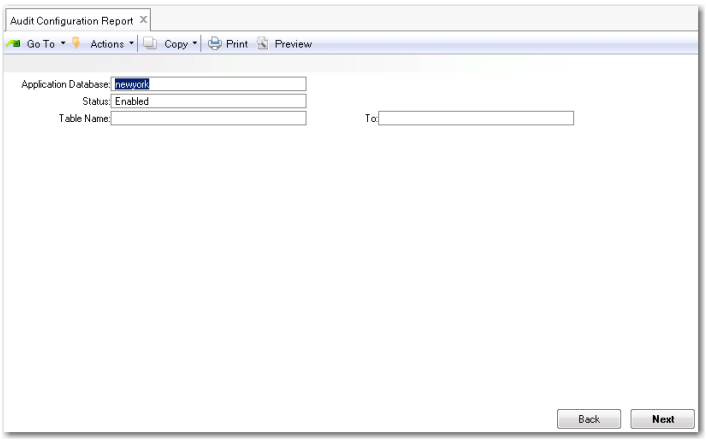
   Note You have to page down in Audit Policy Export to access and select `qadmainpolicy`.

   See “Export Audit Policy” on page 351 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. 13.7
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 Next 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 by entering the following property in the build/config/configuration.properties file:

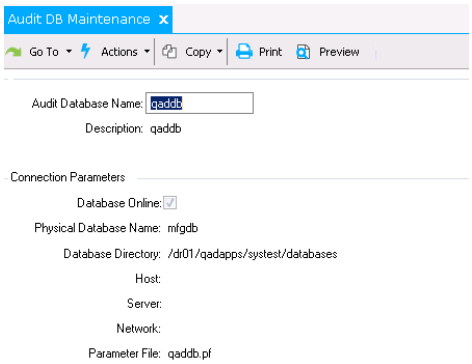
```
dbserver.qadarc.manual=false
```

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. 13.8
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 of eight or fewer characters for this archive database connection record. The name 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 checkbox 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 database security has been enabled as described in “Database Security” on page 43, the parameter file must include the username and password that were used to secure the database. To determine the necessary username and password, enter:

```
yab <db>.connection.user
yab <db>.connection.password
```

Save the user ID and password in a parameter file with the following syntax:

```
-U <username> -P <password>
```

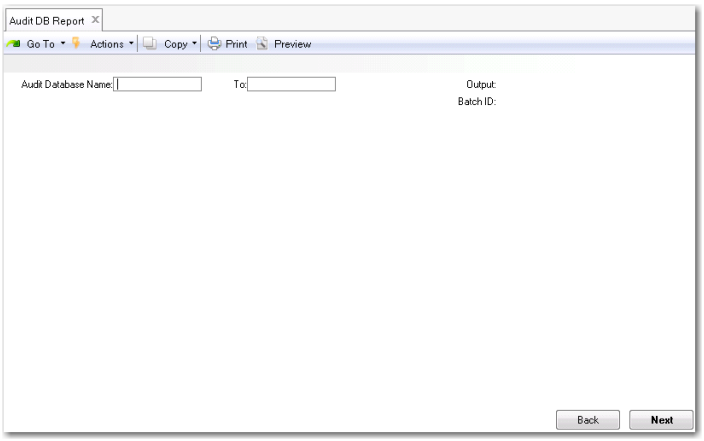
If you use the parameter file:

- 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. 13.9
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 audit trail reports for the main business documents and master tables. These reports show audit trail data from all related tables and provide a complete view of all changes to a document or master table. There is also a generic audit trail report that shows the audit trail data from any arbitrary table.

Document Audit Trail Reports

Document Audit Trail Reports (36.12.12) are a set of reports that provide specific information for each master data area. These reports contain relevant information in an easy-to-read format for business users.

Each report focuses on one main table and its related child tables, linking the information in a single layout. For example, the Supplier Audit Report also includes the auditing information for its child tables, such as supplier domain data and supplier banking information. Similarly, the Sales Order Audit Report includes information for sales order lines, sales order bills, and the comments associated with the orders and lines.

Each report is based on the QAD Reporting Framework and allows for filtering audit trail records based on primary keys, event types (create, modify, delete), dates, and the user who performed the change. Each report offers two output layouts, one for Excel and one for a regular report. The reports display audit events for the tables and fields that have been enabled for auditing through Audit Configuration Maintenance (36.12.13.5) on the Enhanced Controls menu. These reports show audit trail data from the archive database. The available reports are displayed in Table 13.4.

Table 13.4
Document Audit Trail Reports

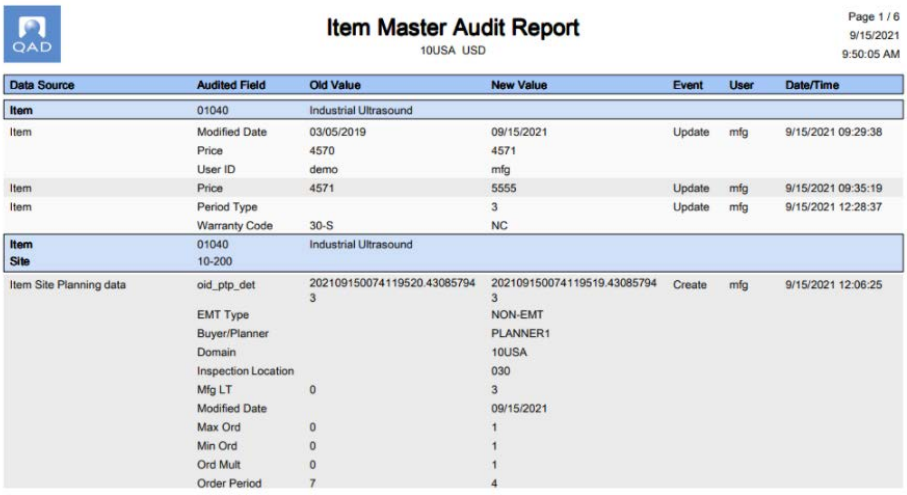
Report	Menu	Master Table	Related Table
GL Account Audit Report	36.12.12.1	GL	Bank Number (BankNumber)
Business Relations Audit Report	36.12.12.2	Business Relation (BusinessRelation)	Address, Contact
Customer Audit Report	36.12.12.3	Customer (Debtor)	Customer Domain Data(cm_mstr), Customer Default SAF's(DebtorSafDefault), Customer Shipto (DebtorShipto), Bank Numbers (BankNumber) Bank Number Payment Formats(BankNumberPayCode)
Supplier Audit Report	36.12.12.4	Supplier (Creditor)	vd_mstr, CreditorSafDefault, Bank Number (BankNumber), Bank Number Payment Formats (BankNumberPayCode)
Customer Invoice Audit Report	36.12.12.5	Customer Invoice (DInvoice)	Customer Bank (DInvoiceBank)
Supplier Invoice Audit Report	36.12.12.6	Supplier Invoice (CInvoice)	Supplier Bank(CInvoiceBank)
Sales (+Scheduled) Order Audit Report	36.12.12.7	Sales Order (so_mstr)	Sales Order Line (sod_det), Sales Order Bill (sob_det), Comments (cmt_det)
Item Master Audit Report	36.12.12.9	Item Master (pt_mstr)	Item Site Planning (ptp_det), Item Site Invnetory (pti_det), Item Cost Total (sct_det), Item Cost Element (spt_det), Supplier Item (vp_mstr)

Report	Menu	Master Table	Related Table
Routing Audit Report	36.12.12.10	Routing(ro_det)	Comments (cmt_det)
Product Structure Audit Report	36.12.12.11	Bill of Material (bom_mstr)	Product Structure (ps_mstr), Item Substitute (pts_det)
Production Order Audit Report	36.12.12.12	Production Order (wo_mstr)	Production Order Component (wod_det), Production Order Routing (wr_route), Comments (cmt_det)
Product Line Audit Report	36.12.12.13	Product Line (pl_mstr)	Product Line Site Inventory (pld_det), Product Line Site Sales (plsd_det), Account Default (acdf_mstr)
Price List Audit Report	36.12.12.14	Price List (pc_mstr)	
Best Pricing Audit Report	36.12.12.15	Price LIst (pi_mstr)	Price List Detail (pid_det), Comments (cmt_det)
Distribution Order Audit Report	36.12.12.16	Distribution Order (dss_mstr)	Distribution Order Line (ds_det), Comments (cmt_det)
User Access Audit Report	36.12.12.17	User Master (usr_mstr)	User Role Entity Access (UsrRoleCompany), User Licensed Application (usrl_det)
Role Resources Audit Report	36.12.12.18	Role (Role)	Role Access Adaptive UX (AccessControlEntry), Role Access Adaptive ERP (RoleResource)

Report Format

All Document Audit Trail reports follow the same format, as shown in Figure 13.10.

Fig. 13.10
Items Audit Trail Report



QAD

Item Master Audit Report
10USA USD

Page 1 / 6
9/15/2021
9:50:05 AM

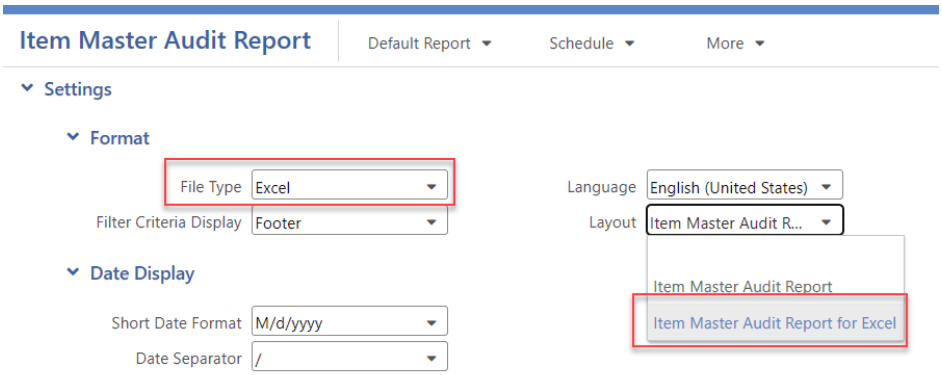
Data Source	Audited Field	Old Value	New Value	Event	User	Date/Time
Item	01040	Industrial Ultrasound				
Item	Modified Date	03/05/2019	09/15/2021	Update	mfg	9/15/2021 09:29:38
	Price	4570	4571			
	User ID	demo	mfg			
Item	Price	4571	5555	Update	mfg	9/15/2021 09:35:19
Item	Period Type		3	Update	mfg	9/15/2021 12:28:37
	Warranty Code	30-S	NC			
Item **Site**	01040 10-200	Industrial Ultrasound				
Item Site Planning data	oid_ptp_det	2021091500741195203.4085794	2021091500741195193.4085794	Create	mfg	9/15/2021 12:06:25
	EMT Type		NON-EMT			
	Buyer/Planner		PLANNER1			
	Domain		10USA			
	Inspection Location		030			
	Mfg LT	0	3			
	Modified Date		09/15/2021			
	Max Ord	0	1			
	Min Ord	0	1			
	Ord Mult	0	1			
	Order Period	7	4			

The Data Source column on the left-hand side and any light blue row together identify a modified record. Events are detailed in the white and gray rows that follow a light blue record row. Each event includes the modified field, the old and new values, the event type, the user who made the change, and the event timestamp.

Excel Output

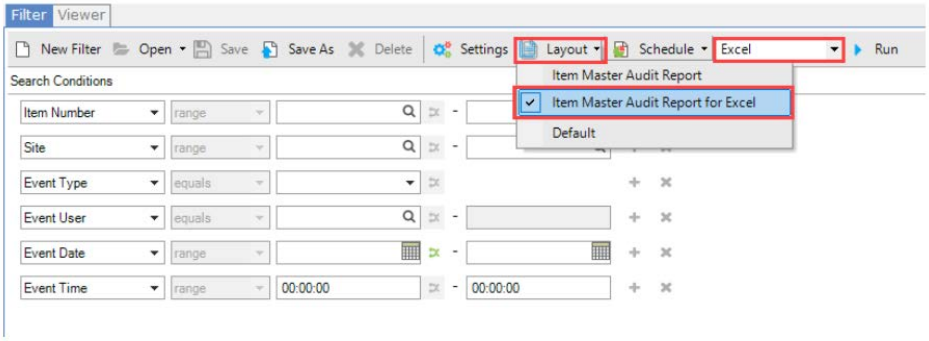
To export an audit report in Excel from Adaptive UX, change the File Type and Layout options on the report screen, as shown in Figure 13.11, and then click Run.

Fig. 13.11
Excel Setup in Adaptive UX



To generate Excel output in Adaptive ERP, you also need to change the Layout and File Type options.

Fig. 13.12
Excel Setup in Adaptive ERP



The output in Excel contains three groupings of columns, as described in the following section. The first group displays the key fields, the second displays the data source and modified fields, and the third group contains the event details.

Key Fields

Fig. 13.13
Excel Output Part 1 - Key Fields

	A	B	C	D	E	F	G	H
1	**Item**	**Description**	**Site**	**Cost Set**	**Element**	**Supplier**	**Supplier Item**	**Data Source**
2	01040	Industrial Ultrasound						Item
3	01040	Industrial Ultrasound						Item
4	01040	Industrial Ultrasound						Item
5	01040	Industrial Ultrasound						Item
6	01040	Industrial Ultrasound						Item
7	01040	Industrial Ultrasound						Item
8	01040	Industrial Ultrasound	10-200					Item Site Planning data
9	01040	Industrial Ultrasound	10-200					Item Site Planning data
10	01040	Industrial Ultrasound	10-200					Item Site Planning data
11	01040	Industrial Ultrasound	10-200					Item Site Planning data
12	01040	Industrial Ultrasound	10-200					Item Site Planning data
13	01040	Industrial Ultrasound	10-200					Item Site Planning data

The Excel spreadsheet includes a column for each key field, highlighted in Figure 13.13 in red. You can identify a record through its key fields and the data source. In the example, for Data Source=Item, you can use the Item Number to identify the record, while for Data Source=Item Site Planning data, you can use the Item Number and Site to identify the record.

Data Source and Modified Fields

Fig. 13.14
Excel Output Part 2 - Data Source and Modified Fields

	H	I	J	K
1	**Data Source**	**Audited Field**	**Old Value**	**New Value**
2	Item	Modified Date	03/05/2019	09/15/2021
3	Item	Price	4570	4571
4	Item	User ID	demo	mfg
5	Item	Price	4571	5555
6	Item	Period Type		3
7	Item	Warranty Code	30-S	NC
8	Item Site Planning data	oid_ptp_det	202109150074119520.430857943	202109150074119519.430857943
9	Item Site Planning data	EMT Type		NON-EMT
10	Item Site Planning data	Buyer/Planner		PLANNER1
11	Item Site Planning data	Domain		10USA
12	Item Site Planning data	Inspection Location		030
13	Item Site Planning data	Mfg LT	0	3

The second group of columns identifies the changed field, along with the previous value and the new value of the field.

Event Details

Fig. 13.15
Excel Output Part 3 - Event Details

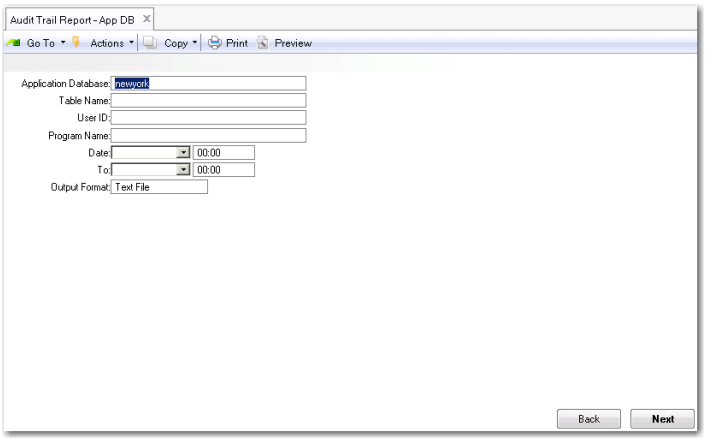
	L	M	N	O	P	Q
1	Event Date	Event Time	Event Type	Event User	Table	Field
2	9/15/2021	09:29:38	Update	mfg	pt_mstr	pt_mod_date
3	9/15/2021	09:29:38	Update	mfg	pt_mstr	pt_price
4	9/15/2021	09:29:38	Update	mfg	pt_mstr	pt_userid
5	9/15/2021	09:35:19	Update	mfg	pt_mstr	pt_price
6	9/15/2021	12:28:37	Update	mfg	pt_mstr	pt_period_type
7	9/15/2021	12:28:37	Update	mfg	pt_mstr	pt_warr_cd
8	9/15/2021	12:06:25	Create	mfg	ptp_det	oid_ptp_det
9	9/15/2021	12:06:25	Create	mfg	ptp_det	ptp_btb_type
10	9/15/2021	12:06:25	Create	mfg	ptp_det	ptp_buyer
11	9/15/2021	12:06:25	Create	mfg	ptp_det	ptp_domain
12	9/15/2021	12:06:25	Create	mfg	ptp_det	ptp_insp_loc
13	9/15/2021	12:06:25	Create	mfg	ptp_det	ptp_mfg_lead

The final columns display the technical table and field names, along with the Event Type, the user who made the change, and the event date and time.

Generate Reports Against Application Databases

You can generate auditing reports against the application databases using Audit Trail Report–App DB (36.12.1).

Fig. 13.16
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.

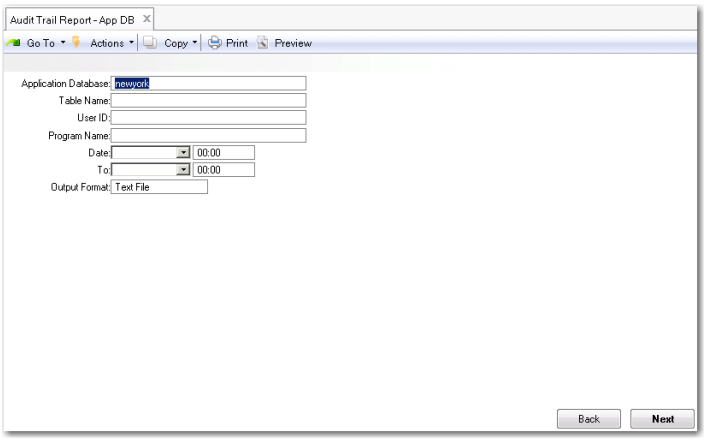
Summary/Detail. Select summary mode or detail mode. In summary mode, no field value changes are reported.

Output Format. Specify the output format as a text file (`.txt`), XML file (`.xml`), or CSV file (.csv).

Note The CSV file option generates a comma-separated list that can be imported into most spreadsheet applications.

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. 13.17
Audit Trail Report–App DB Field Selection



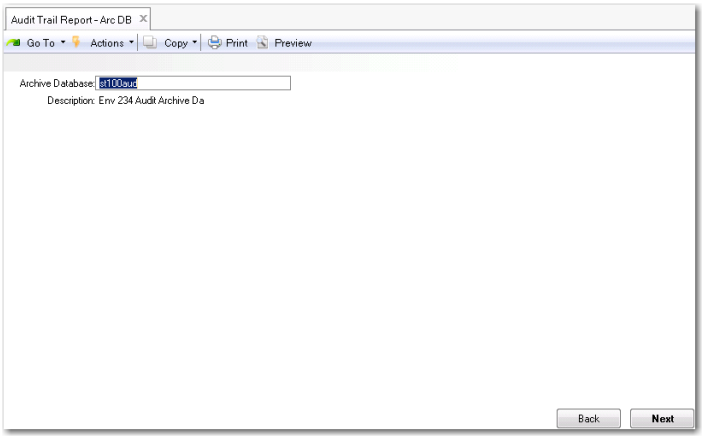
Click Next again to have the system retrieve the records according to the criteria you have specified and generate a report (or output file).

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. 13.18
Audit Trail Report–Arc DB (36.12.2)



To generate audit reports, specify the following:

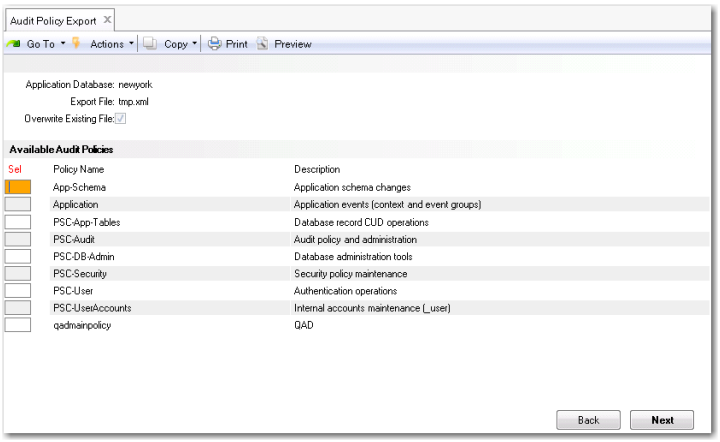
Archive Database. Select one of the archive databases. If the database selected is not enabled for auditing, the system displays an error message. Use Audit DB Maintenance (36.12.13.11) to define archive database information.

Click Next to have the system retrieve the records according to the criteria you have specified and generate a report or output file. You can choose to save the data to a CSV file, which generates a comma-separated list that can be imported into most spreadsheet applications.

Export Audit Policy

You can export current audit policies to Progress policy XML files using Audit Policy Export (36.12.13.2).

Fig. 13.19
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
```

Chapter 14

Reverse Proxy for QAD Adaptive ERP

This section covers the following topics:

Overview ***354***
Explains the security benefits of using a generic proxy.

Configuration ***354***
Explains how to configure the proxy controller.

Configuring Apache Reverse Proxy Timeout Setting ***358***
Explains how to configure Apache Reverse Proxy Timeout Setting.

Configuring Caching of Java Objects ***358***
Explains how to configure Caching of Java Objects.

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 Adaptive UX controls access to those applications.

Configuration

The Proxy Controller is configured with property updates to the `build/config/configuration.properties` file. After these updates are complete, you must run a yab update for the changes to take effect.

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 14.1
Proxy Configuration

Property	Description
qad-webshell.proxy.names	Comma-separated list of proxy names. These are then used as keys for the other properties in this table.
qad-webshell.proxy.{name}.proxyFrom	The path from which to proxy; for example, /remote must start with a /. The full proxy path is generated from this value as /{context}/proxy{proxyFrom}.
qad-webshell.proxy.{name}.proxyTo	The URL to which to proxy; for example, https://remote.qad.com/context.

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\(\s*'(?:https://remote\.qad\.com/path|/path)((?:[^'\\]|\\.)*)'\s*\) -> url('/qad-webshell/proxy/app$1')
url\(\s*"(?:https://remote\.qad\.com/path|/path)((?:[^"\\]|\\.)*)"\s*\) -> 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 14.2
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'
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)((?:[^"\\\\]|\\\\.)*)' '/qad-webshell/proxy/app$1' \"(?:https://remote\.qad\.com/path|/path)((?:[^"\\\\]|\\\\.)*)\" "/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/

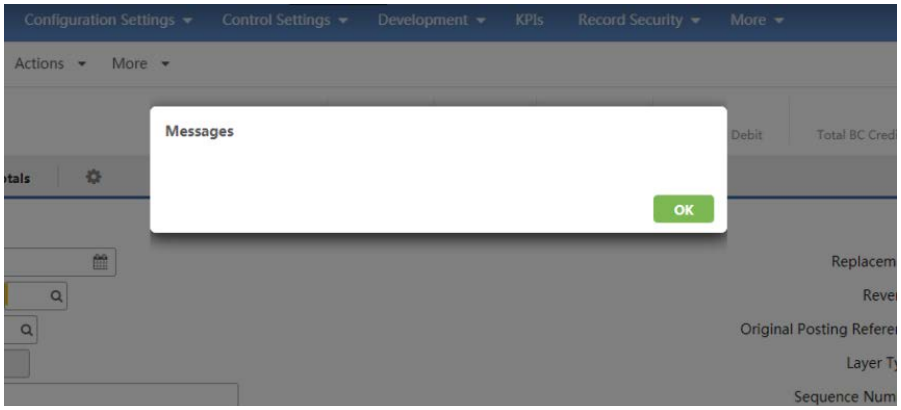
The Tomcat proxy has URL rewriting enabled for HTML links with custom attributes and mappings. The `build/config/configuration.properties` file would look like the following:

```
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 Apache Reverse Proxy Timeout Setting

QAD recommends increasing the timeout setting for environments using an Apache Reverse Proxy. The default timeout setting is not sufficient to allow some areas of the Adaptive UX, such as reports, to complete requests before timing out. When the Apache Reverse Proxy times out, the system can return blank error messages, as in Figure 14.1.

Fig. 14.1
Blank Message



If you select OK in the blank message, a record with empty fields opens instead of the record with which you were working. You can continue to work with the system, but the timeout can happen again after you re-enter the data on the screen.

To avoid this scenario, increase the Proxy Timeout value in the `httpd.conf` file. For example, to set the timeout to 20 minutes, enter:

```
ProxyTimeout 1200
```

Once this change is made, restart the Apache server. This is done outside of YAB, with no need to restart Tomcat or any other component of QAD Adaptive ERP.

Configuring Caching of Java Objects

Adaptive UX 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 `build/config/configuration.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.

Chapter 15

Menu Search Implementation

This section covers the following topics:

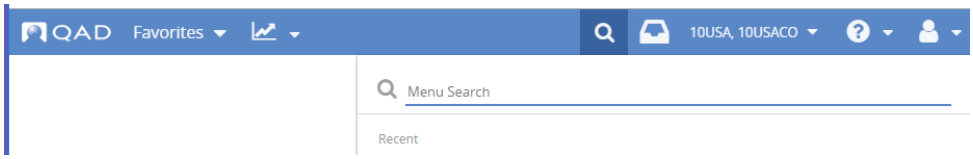
Overview ***362***
Explains the two search implementations for Adaptive UX.

Elasticsearch Settings ***362***
Explains how to enable Elasticsearch for the Menu Search in Adaptive UX.

Overview

The Menu Search in Adaptive UX is located in the Menu Bar and expanded by selecting the magnifying glass icon. It helps users find all of the menu items available to them. For detailed information on the Menu Search, see the Adaptive UX online help, located under the question mark icon in the Menu Bar.

Fig. 15.1
Menu Search



Menu Search can be enabled using either Elasticsearch or an Ehcache implementation, with Elasticsearch enabled by default.

Elasticsearch Settings

Table 15.1 explains the default Elasticsearch properties. To update any of these parameters, you must enter the new property setting in the `configuration.properties` file.

Table 15.1
Elasticsearch Properties Configuration

Property	Description
qad-qraview.search.elastic.enabled	Defines if Elasticsearch is enabled. Set to true by default. (Required)
qad-qraview.search.elastic.address	Defines the Elasticsearch server address in the form ${elasticsearch.default.url} (Required)
qad-qraview.search.elastic.resultSize.documents	Defines the number of documents returned from the Elasticsearch engine. Defaults to 250.
qad-qraview.search.indexPeriod.seconds	A number of seconds, representing the time between document reindexing. Defaults to 84600 (one day).

To disable Elasticsearch and use Ehcache for searches, set `qad-qraview.search.elastic.enabled=false`.

Note The Ehcache implementation uses only the local Tomcat server to return results and does not handle large numbers of documents as well as Elasticsearch.

Troubleshooting

Use the following information to troubleshoot an Elasticsearch implementation.

Correct Initialization Logs

Ensure that Elasticsearch initialized correctly. In the logs directory, check `catalina.out` by entering:

```
grep -i 'indexService\|indexBuilder\|engineClient\|retriever' catalina.out
```

You should see something similar to:

```
[19/05/10@00:49:11.624-0700] INFO   com.qad.qraview.search.IndexService: Start bulk adding
of documents to index with name='menu_item-en'
[19/05/10@00:49:11.866-0700] INFO   com.qad.qraview.search.ElasticEngineClient: Index with
name='menu_item-en' deleted successfully
[19/05/10@00:49:12.032-0700] INFO   com.qad.qraview.search.ElasticEngineClient: Index with
name='menu_item-en' created successfully
[19/05/10@00:49:15.074-0700] INFO    com.qad.qracore.search.MenuItemRetriever: '1554' menu
items were retrieved from DB
[19/05/10@00:49:15.133-0700] INFO   com.qad.qraview.search.MenuItemIndexBuilder: Query for
bulk indexing created for index with name='menu_item-en'
[19/05/10@00:49:15.622-0700] INFO    com.qad.qraview.search.ElasticEngineClient: '1554'
documents added successfully to index with name='menu_item-en'
[19/05/10@00:49:15.622-0700] INFO   com.qad.qraview.search.IndexService: Finish bulk adding
of documents to index with name='menu_item-en'
```

This example shows a system in which only English is configured. If multiple languages are configured in your system, you will see similar results for all languages.

Incorrect Initialization Logs

You can determine if the Elasticsearch server is not started but the Tomcat server is running. In the logs directory, check `catalina.out` by entering:

```
grep -i 'indexService\|indexBuilder\|engineClient\|retriever' catalina.out
```

You will see output similar to the following example. Look for these types of errors.

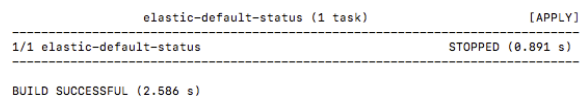
```
[19/05/10@06:58:59.932-0700] ERROR   com.qad.qraview.search.ElasticEngineClient: Cannot
connect to Elasticsearch node with URL='http://localhost:22171/menu_item-en', method='HEAD'
[19/05/10@06:58:59.946-0700] ERROR   com.qad.qraview.search.ElasticEngineClient: Cannot
connect to Elasticsearch node with URL='http://localhost:22171/menu_item-en', method='PUT'
[19/05/10@06:58:59.946-0700] ERROR   com.qad.qraview.search.ElasticEngineClient: Index with
name='menu_item-en' NOT created
[19/05/10@06:59:02.892-0700] INFO    com.qad.qracore.search.MenuItemRetriever: '1555' menu
items were retrieved from DB
[19/05/10@06:59:02.960-0700] INFO   com.qad.qraview.search.MenuItemIndexBuilder: Query for
bulk indexing created for index with name='menu_item-en'
[19/05/10@06:59:02.962-0700] ERROR   com.qad.qraview.search.ElasticEngineClient: Cannot
connect to Elasticsearch node with URL='http://localhost:22171/_bulk', method='POST'
[19/05/10@06:59:02.963-0700] ERROR   com.qad.qraview.search.ElasticEngineClient: NO
documents added to index with name='menu_item-en'
[19/05/10@06:59:02.963-0700] INFO   com.qad.qraview.search.IndexService: Finish bulk adding
of documents to index with name='menu_item-en'
```

Check the Elasticsearch status.

```
yab elastic-default-status
```

You should see something similar to Figure 15.3.

Fig. 15.2
Elasticsearch Stopped



If the default status is STOPPED, start Elasticsearch with the command `yab elastic-default-start`. Then restart Tomcat with the command `yab tomcat-webui-stop tomcat-webui-start`.

No Results Returned

If users are trying to perform menu searches and no results are found for any search query, the Elasticsearch server is not running. You can see errors in the `catalina.out` log file similar to the following:

```
[19/05/10@07:10:17.099-0700] ERROR mfg  com.qad.qraview.search.ElasticEngineClient: Cannot connect to Elasticsearch node with URL='http://localhost:22171/menu_item-en/_search', method='GET'
```

Check the Elasticsearch status.

```
yab elastic-default-status
```

You should see something similar to Figure 15.3.

Fig. 15.3
Elasticsearch Stopped

```
                elastic-default-status (1 task)                    [APPLY]
--------------------------------------------------------------------------------
1/1 elastic-default-status                              STOPPED (0.891 s)
--------------------------------------------------------------------------------

BUILD SUCCESSFUL (2.586 s)
```

If the default status is STOPPED, start Elasticsearch with the command `yab elastic-default-start`. Then restart Tomcat with the command `yab tomcat-webui-stop tomcat-webui-start`. Menu Search now should return results.

Appendix A

KMS Backup and Recovery

This appendix describes the critical steps required to back up and restore your key management service.

Overview

The KMS can become corrupt or unavailable for a number of reasons, such as hardware failure, user error, or DOS attack. Because the KMS plays a vital role in normal operations, it is important you can restore service to the existing KMS or configure a new instance. You should periodically validate your backup and restore process in any production environment.

KMS Backup

Two files are necessary for a successful backup and recovery scenario:

- `kms-backup-[date and time].zip`
- Data file defined by the YAB property `kms.data.file`

Important It is your responsibility to save copies of the KMS backup files and store the copies in a secure location on a separate host from your environment. Failure to save a copy of the latest KMS backup zip file could lead to catastrophic consequences for your system. If your system fails and you do not have these files, any information that was encrypted would not be recoverable.

KMS Zip File

There are two default configuration properties for KMS backups, which are described in the following table.

Table 0.1
KMS Backup Properties

Property	Description	Example
kms.backup.dir	The backup directory.	kms.backup.dir= /directory/servers/kms/backup
kms.backup.schedule.seconds	The amount of time in seconds between KMS checking if a backup is required. Default is 86400 (24 hours).	kms.backup.schedule.seconds= 86400

The key management service saves a backup of critical information to a zip file, `kms-backup-[date and time].zip`, in the backup directory. The KMS saves an initial backup when the service is created and then only generates a new zip file if the backup file is missing from the backup directory or if there have been changes to any of the files in its storage directory. The KMS checks for changes or a missing file based on the `kms.backup.schedule.seconds` property, which is set to 24 hours by default.

Data File

You also need to save a copy of the data file defined by the property `kms.data.file`, which contains client credentials and an encryption keyring. The `kms.data.file` is located by default in `servers/kms/kms-local.properties`. This file is created by YAB and contains settings that are important to communicate with the KMS because they cannot be regenerated.

KMS Recovery

Before beginning the restore process, it is recommended you create a copy of the existing KMS storage area before restoring the backup over it.

1. Ensure the KMS is no longer running.

   ```
   yab kms-stop
   ```

2. Find the most recent backup file, defined through `kms.backup.dir`. If you are testing in a functional environment, you can find the backup file by entering:

   ```
   ls -tr servers/kms/backup
   ```

3. Locate the KMS storage directory.

   ```
   yab config kms.storage.dir
   ```

4. Unzip the backup file to the KMS storage directory you located in step 3.

5. Start the KMS.

   ```
   yab kms-start
   ```

6. Verify encryption and decryption are working as expected. You can do this by encrypting a text string and ensuring the KMS returns encrypted content. For example, enter:

   ```
   yab kms-encrypt foo
   ```

   The command should return {`cipher`} followed by a string of letters and numbers that is the encryption of `foo`.

Appendix B

Logi Platform Services

Logi Platform Services powers the Action Centers and analytics in Adaptive UX. This appendix describes the steps required to make Logi Platform Services active in your system.

Logi Platform Services Network Ports ***370***

HTTPS Certificates ***371***

Apache Reverse Proxy Configuration for LogiPS ***371***

Logi Platform Services Product Database Security ***372***

Logi Platform Services Network Ports

Various network ports required by Logi Platform Services (LogiPS) are automatically configured by YAB. These ports have different purposes within the Logi architecture with different security considerations. The HTTPS and HTTP service ports are external to LogiPS and are accessed from the tomcat-webui server. The remaining ports are internal to LogiPS. None of the ports require direct access by client browsers.

The ports are summarized in the following table.

YAB Property	Purpose of Port and Required Access to Port	Security Approach	Remarks
logi-platform-services.default.service.application.webserver.sslport	HTTPS client access to LogiPS tomcat-webui server of Adaptive UX only	Native Logi Platform (native user) authentication and Adaptive UX (trusted user) authentication	Used for Logi Platform API access.
logi-platform-services.default.service.application.webserver.port	HTTP client access to LogiPS tomcat-webui server of Adaptive UX only	Native Logi Platform (native user) authentication and Adaptive UX (trusted user) authentication	Used for Logi Platform API access, but disabled by default in favor of HTTPS.
logi-platform-services.default.service.data.h2.port	H2 (PDB) database access Internal to LogiPS	Internal username-password credentials, automatically configured by LogiPS and not managed by YAB	Internal to Logi Platform. See “Logi Platform Services Product Database Security” on page 372 for more details.
logi-platform-services.default.service.data.ldap.port	Embedded LDAP access Internal to LogiPS	Configurable username-password credentials, with password encrypted in file by LogiPS and not managed by YAB	Internal to Logi Platform. Rarely a need to change password.
logi-platform-services.default.service.data.stomp.port	ActiveMQ access - Stomp Internal to LogiPS	Internal username-password credentials, automatically configured by LogiPS and not managed by YAB	Internal to Logi Platform. Rarely a need to change password.
logi-platform-services.default.service.data.openwire.port	ActiveMQ access - Openwire Internal to LogiPS	No authentication is needed. Protocol is binary and communications are internal to ActiveMQ transport within LogiPS	Internal to Logi Platform. Rarely a need to change password.

HTTPS Certificates

LogiPS is installed by default in Adaptive UX to be accessed using HTTPS, and must be configured to avoid network security errors raised at run time when Adaptive UX is also set up to be accessed through HTTPS.

Creating HTTPS Certificates

To use HTTPS with Logi Platform Services, a public certificate file and a private key file are required in the PEM format, which is a common standard for storing cryptographic data. The certificate and key files in the Java Keystore (JKS) format used by Tomcat do not work with Logi Platform Services. You must either generate new files in the PEM format, or convert existing JKS certificate and key files to that format.

Certificate and key files are not included in the QAD Adaptive ERP installation and are not generated by YAB. They can be created on-site specifically for each company that is installing the software or procured through a CA. They can be created in different ways, and there is no prescribed procedure. Follow your company's guidelines for obtaining a certificate in PEM format.

Configuring Certificate Files and Location

Once the certificate files are available, they must be placed in a fixed location on the file system where they can be read by YAB and copied into the Logi Platform Services installation. Various YAB properties must be set describing the files so that Logi Platform Services can consume them. The required properties are described in the following table.

Define these properties in the `configuration.properties` file.

Property Name	Description	Default Value
logi-platform-services.default.sourcekeyfile	Full path of the filename containing the private key to be used by LogiPS.	N/A
logi-platform-services.default.sourcecertfile	Full path of the filename containing the public certificate to be used by LogiPS.	N/A
logi-platform-services.default.selfsigned	Indicates if the certificate is self-signed.	false

Apache Reverse Proxy Configuration for LogiPS

Many Adaptive ERP installations deploy an Apache web server as a reverse proxy in front of the Tomcat container to intercept and forward all web requests through a single port exposed to the internet. In environments in which an Apache reverse proxy is being used, a particular configuration change is required to support Logi Platform Services correctly.

In Adaptive ERP installations, the Apache configuration files contain a Location element that references the URL path of the reverse proxy. The following example environment references the reverse proxy `clouderp`.

```
<Location /clouderp>
    ProxyPass https://vmlqad0000.qad.com:22011/qad-central
    ProxyPassReverse https://vmlqad0000.qad.com:22011/qad-central
    Header edit Set-Cookie "^(.*)/qad-central(.*)$" $1/clouderp$2
    Header edit Location "/qad-central/"
    "https://vmlxxx0000.qad.com/clouderp/"
    AddOutputFilterByType SUBSTITUTE text/html image/svg+xml
    Substitute "s|/qad-central|/clouderp|iq"
    Substitute "s|https://vmlqad0000.qad.com:22011|
    https://vmlqad0000.qad.com|iq"
</Location>
```

In order to support Logi Platform Services, update the AddOutputFilterByType element in the previous example to the following, adding the MIME type `application/com.qad.webshell.proxy+json` to the end.

```
AddOutputFilterByType SUBSTITUTE text/html image/svg+xml
application/com.qad.webshell.proxy+json
```

Once this change is made, restart the Apache server. This is done outside of YAB, with no need to restart Tomcat or any other component of QAD Adaptive ERP.

Logi Platform Services Product Database Security

Logi Platform Services includes a separate product database (PDB), which it uses instead of storing all information inside individual XML files saved in the file system. This product database contains internal representations of the Action Centers, visuals, and KPIs, in addition to system configuration data. It is relational and implemented using the H2 database engine. The Logi Data Service within LogiPS connects to the PDB through a single configurable port, secured with login credentials.

The PDB is not accessed outside of LogiPS. Neither YAB nor Adaptive UX ever reads or writes its contents directly, and there is no reason for its connection port to be exposed outside of the enterprise firewall. While this port can be configured by YAB, the database connection credentials are native to LogiPS and not maintained using YAB.

The port used by the PDB for client connections is stored in the following YAB property, dynamically assigned by YAB at installation time.

```
logi-platform-services.default.service.data.h2.port
```

The PDB connection credentials are automatically set by LogiPS at installation time and should never need to be changed. However, LogiPS provides a command line utility `dbPassword.sh` that can be used to change them if needed. Following is the help text for using this utility:

```
dbPassword: Change platform MQ or DB password
Usage

-v, --verbose <number>    Provide extensive output (0-3)
--help                    Print usage instructions
-o, --offline             Invoke command in offline mode
-c, --MQ                  Change Message Queue password
-d, --DB                  Change Database password
```

The `-d` option is used to change the PDB password. Logi Platform Services should be stopped before using the utility. After the utility is run, Logi Platform Services must be restarted.

Index

Symbols

! (exclamation point) 182
.NET UI security 26
* (asterisk) 182

Numerics

2.14.1 108
36.3.1 106
36.3.3 21
36.3.4 115
36.3.6.1 93
36.3.6.2 93
36.3.6.3 93
36.3.6.4 94
36.3.6.5 14, 101, 224, 260
36.3.6.6.1 15, 119
36.3.7.1 190
36.3.7.2 191
36.3.7.3 192
36.3.7.5 193
36.3.7.6 193
36.3.7.8 194
36.3.7.9 195
36.3.7.13 195
36.3.7.14 195
36.3.7.15 196
36.3.7.17 196
36.3.13.1 197
36.3.13.2 197
36.3.13.8 186
36.3.13.13 198
36.3.13.14 198
36.3.15.1 184, 185
36.3.15.2 185
36.3.15.3 183
36.3.15.4 184
36.3.22 115
36.3.23.1 19, 35
36.3.23.12 112
36.3.24 28
36.5.3.24 182
36.12.4 305
36.12.5 306
36.12.7 307
36.12.1 349
36.12.13.8 283, 299
36.12.13.1 337
36.12.13.11 341, 343, 351
36.12.13.12 343
36.12.13.2 351
36.12.13.5 338, 339
36.12.13.7 339
36.12.14.1 293
36.12.14.4 283, 293
36.12.14.5 295
36.12.14.9 300
36.12.14.21 307
36.12.14.22 283, 309
36.12.14.23 283, 309
36.12.2 341, 350
36.16.10.1 115
36.24.1 19
36.6.1 341

A

actions
  Sync Users 67
Activated E-Signature Profile Report 300
Activated Field Security Report 183
Active Directory user sync 65
Active field 110
address
  e-mail specification 110
administrator
  security e-mail 34
Administrator Role field 30
Apache Cassandra 53
Apache Kafka 51
Apache Reverse Proxy
  LogiPS 371
  timeout 358
API authentication 69
API type
  User Maintenance 110
application resource 3
applications
  assigning 114
AppServerDCS xiii, 47, 48
Archive SOD log records 239, 275
archive/delete
  electronic signature failures 307
  electronic signatures 283, 309
Assigning segregation of duties categories 218, 257
Audit Configuration Field Level 339
Audit Configuration Maintenance 338, 339
audit databases
  archiving electronic signatures 309
Audit DB Maintenance 341, 343, 351
Audit DB Report 343
Audit Policy Export 351
Audit Policy Import 337
audit profiles

groups 293
overview 292
Audit Trail Report - App DB 349
Audit Trail Report - Arc DB 341, 350
auditing 330
role permissions 155
roles 123
user access 125
user licenses 124
users 124
Auto-Disablement Reason field 31

C
Cassandra 53
categories, electronic signature 285
certificate for SSL 39
checklists
security implementation 7
client ID 77
client secret 77
committing data to database 302
compiles
protecting in Progress 23
component-based functions 3
control programs
security 28
country
information in locale.dat file 108
setting country code for user 108
Country Code Data Maintenance 108
County Code field 108
Ctrl+F display 30
Current field 300
Customer type
User Maintenance 109

D
data
committing to database 302
Data Administration (Progress) 334
data dictionary
field security 184
Database Connection Maintenance 341
Database Control 19
database security 43
databases
Progress security 23
DBAUTHKEY function in Progress 24
deactivated roles 94
default domain 117
default role 89
delete/archive
electronic signature failures 307
electronic signatures 283, 309
dependencies 143
Dictionary Field Security Report 183, 184
Directory Services Markup Language Service 58
DO Receipts Restriction Maintenance 196
DO Restriction Maintenance 195
DO Shipments Restriction Maintenance 195
domains
default 117
security access 18, 115
DSML 58
install DSML gateway 59

E
electronic signature categories 285
electronic signature profiles
activating 299
refreshing 293
updating in workbench 295
electronic signatures 278, 309, 312
Adaptive UX 311
Web UI 311
e-mail
auditing notifications 303
electronic signature notifications 284, 315
notification settings 30
security notifications 34
user's address 110
employee type
User Maintenance 109
enabled reason code 112
Enabled Reason field 112
Enabled Reason Type field 31
Enabled setting 112
Enforce Licensed User Count 29, 114
Enforce OS User ID 29
Enhanced Controls license 330
entity security 115, 116
errors
license violations 29
E-Sig Failure Archive/Delete 307
E-Signature Archive/Delete 283, 309
E-Signature Events Report 305
E-Signature Failure Report 307
E-Signature Group Maintenance 293
E-Signature History Report 306
E-Signature Profile Activation 283, 299
E-Signature Restore 283, 309
E-Signature Workbench Profile Maintenance 295
E-Signature Workbench Refresh 283, 293
exceptions
segregation of duties policy 225, 262
SOD policy 225, 262
Export SOD data to Excel 231
Export SOD data to XML 234

F
favorites menu 133
field security 183
validation 184
Field Security by Role 185
Field Security Maintenance 184, 185
filters, electronic signature 289, 297, 299
Force Password Change field 112
Force Password Change Utility 112
functions
component-based 3

G
general ledger (GL)
account security 197
GL Account Security Maintenance 197
GL Account Security Report 197
gppswd.v 184
groups

auditing 293
electronic signature 293

H
Header Display Mode field 29

I
Import SOD data from Excel 232
Import SOD Data from XML 235
inactive records 110
interface preferences 111
International Organization for Standardization (ISO) codes 108
Inventory Detail Restriction Maintenance 191
Inventory Movement Code Security 198
Inventory Movement Code Security Browse 198
Inventory Transfer Restriction Maintenance 190
inventory update 185–197
Invoice Post
site security 186

K
Kafka 51
key management service 42
keystore 39

L
Language field
User Maintenance 108
languages
identifying for users 108
LDAP
attribute listing 63
configure instance 65
set up multiple services 60
LDAP authentication 58
length
password minimum 32
License Registration 115
licensing
interaction with User Maintenance 114
tracking violations 29
warnings versus errors 29
locale.dat file 108
log files
segregation of duties 239, 275
Logon Attempt Report 19, 35

M
material requirements planning (MRP)
site security 186
Maximum Access Failures field 30
membership
role 15, 119
menu
favorites 133
menu substitution
User Maintenance 111
menu-eligible resource 129
menus 129
role 129
Mobile App 118

N
.NET UI security 26
Nifi 55
node states 103

O
operating system
security 22–??
using ID for application sign in 20
Operational Transaction Post 116

P
parameter file 342
passwords
creation method 33
forcing change 112
managing 17
Security Control settings 32
updating 113
permissions
assigning 146
granting access to screens 146
missing 146
role 14
permissions grid 142
permissions tree search 141
PO Receipts Restriction Maintenance 193
PO Restriction Maintenance 193
Primary location for user access 110
Product Change Control (PCC)
using electronic signatures with 302
programs
standard 3
Progress
blank user ID 23
compiles, protecting 23
database schema controls 23
DBAUTHKEY function 24
Editor security 22
RCODEKEY function 24
schema controls 23
security 22
Progress Editor
access 22

Q
QAD Adaptive UX
user access 118
QAD type
User Maintenance 109
QAD Web UI
assign roles 120
favorites menu 133
menus 129
permissions grid 142
resource dependencies 143
role menus 129
role permissions 136

R
RCODEKEY function in Progress 24
reason codes
active reason 31
electronic signatures 283, 314

enabled reason 112
record-level security 158
record-locking during signature entry 296
records
active 106
inactive 110
registered applications
assigning 114
reports
electronic signatures 305
resource
application 3
resource dependencies 143
Resource spreadsheet 230
role context 119
Role Create 93
Role Delete 94
role membership 15
role membership compliance 202, 244
Role Membership Maintain 15, 119, 225
role menu 129
Role Modify 93
role permissions 136
permissions tree 141
role permissions compliance 202, 244
Role Permissions Maintain 14, 101, 224, 260
Role View 93
role-based access control 14–??, 86
roles 14, 88
deactivated records 94
default 89
deleting 94
system-supplied 92

S

Sales and Use Tax Interface (SUTI)
controlling access 182
SAML SSO 74
SAML endpoints 78
troubleshooting 81
Sarbanes-Oxley (SOX) Act 2
schema
controlling in Progress 23
search UserID 69
secure records
change ownership 170
secured resources 128
security
AppServerDCS xiii, 47, 48
Cassandra 53
client level 25
data in transit 49
Dictionary Field Security Report 183
domain 18
field 183
field limitations 184
GL accounts 197
implementation checklists 7
implementation summary 6
inventory movement code 198
Kafka 51
monitoring 35
Nifi 55
overview 3
Progress Editor 22
schema level 23
site 186
special characters 182
types of 4
wild cards 182
Windows systems 25
security contexts 68
Security Control 28
security groups 161
security rules 165
segregation of duties (SOD)
planning SOD system 205, 247
setup workflow 203, 245
Segregation of duties categories 214
definition 202, 244
Segregation of duties matrix 221
Segregation of Duties Menu 203, 245
Session Expires Minutes field 29
sign in
security 18
tracking attempts 35
using operating system user ID 20
signature meaning 283, 314
single sign-on
QAD .NET UI 79
SAML 74
site security 186
excluded functions 186
ranges of sites 187
setting up 187
Site Security Maintenance 186
smart card authentication 70
SO Restriction Maintenance 194
SO Shipments Restriction Maintenance 195
SOD Block All Rule Violations 222
SOD Block All Rule Violations field 202, 206, 207, 208, 213, 228
SOD Block All Violations field 222
SOD Category Create 214
SOD Category Delete 215, 216
SOD Category Excel Integration 216
SOD Category Membership Maintain 218, 220
SOD Category Modify 215
SOD Category View 215
SOD Category worksheet 216, 229
SOD Configuration 202, 206, 207, 208, 212, 222, 228
SOD Import/Export 228
SOD Log Archive 239
SOD Log Delete/Archive 239, 275
SOD Log Viewer 235, 239
SOD Matrix Maintain 221
SOD Matrix worksheet 229
SOD Policy Exception Create 225, 262
SOD Policy Exception Delete 227
SOD Role Exclusion 227
SOD Role Permissions Comparison Report 261
SOD Violations Rule 1 View 238
SOD Violations Rule 2 View 238
SSL 40
SSM Restriction Maintenance 196
standard programs 3
states
node 103

stored view access 157
Sync Users 67
System Access frame
  User Maintenance 111
system roles 92

T
Tax Interface Control 182
time zone
  setup 110
Time Zone field 110
Timeout Minutes field 25, 28
top tables, electronic signature 289
tracking
  sign-in attempts 35
transaction scoping 302
Transparent Data Encryption 45
tree nodes 103
troubleshooting
  permissions 146
  SAML SSO 81
truststore 39

U
Unplanned Issue/Receipt Restriction Maintenance 192
update restrictions 187
  wildcards 188
Update Search Filter 68
Update Search Root 68
user access 118
User Access by Application Inquiry 115
user authentication 58
User Domain/Entity Access Maintain 115
user ID
  assigning 106
  blank, in Progress 23
  displaying at user interface 30
  setting up 106
User Maintenance 106
  country code 108
  interface preferences 111
  language 108
  locale 108
  QAD type 109
  System Access frame 111
  time zone 110
  Variant field 108
user name
  viewing 30
User Password Maintenance 21
user sync 65
User Type field 109
Users
  Sync Users 67
users
  defining types 110
  e-mail address 110
  enforcing license agreement 114
  interface preferences 111
  locale 108
  mobile 118
  time zone 110
  violation messages for license agreement 114

V
Variant field
  User Maintenance 108

W
warning messages
  license violations 29
wildcards
  update restrictions 188
  use with security 182
Windows security options 25
workflow
  electronic signatures setup 281, 312
  security setup 6
  segregation of duties setup 203, 245
workspace security 18

X
X.509 certificate 39