Security Administration Guide

QAD Adaptive Applications

70-3349-QADAdaptive2025
QAD Adaptive 2025
November 2025

Security_AG_QADAdaptive_v2025.pdf/sti/ymg/su9

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

Contents

Security Admin Guide Change Summary

Change Summary

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

Date/Version	Description	Reference
November 2025/QAD Adaptive	Restructured the guide for the new QAD Adaptive product – initial publication.	--

Chapter 1

Introduction to Security

This section introduces the security and internal control features 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 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 is 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 can also 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, System Administrator must configure security for such add-on products appropriately. These security details are included in the relevant product documentation of the other components.

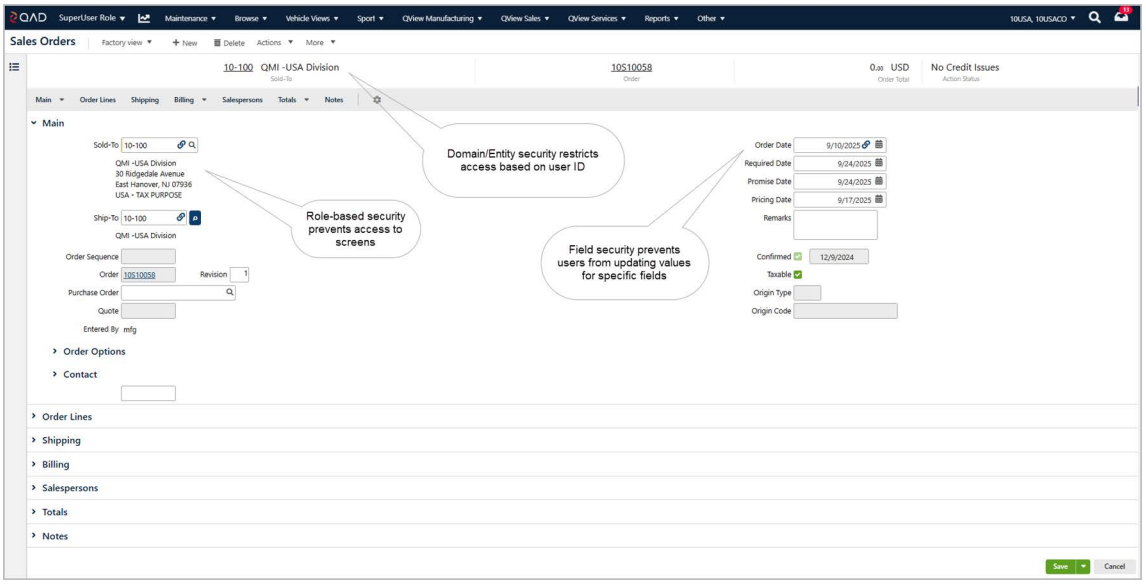
Additionally, QAD Adaptive is comprised of multiple types of resources, each uniquely identified and marked as requiring security. These resources include business entities, services, browses, fields, and KPIs.

When a user logs in, the system determines programs and functions to display on the application menu based on the user's roles in the current domain and entity.

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 23 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.
- 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 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 QAD Adaptive.
- 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:

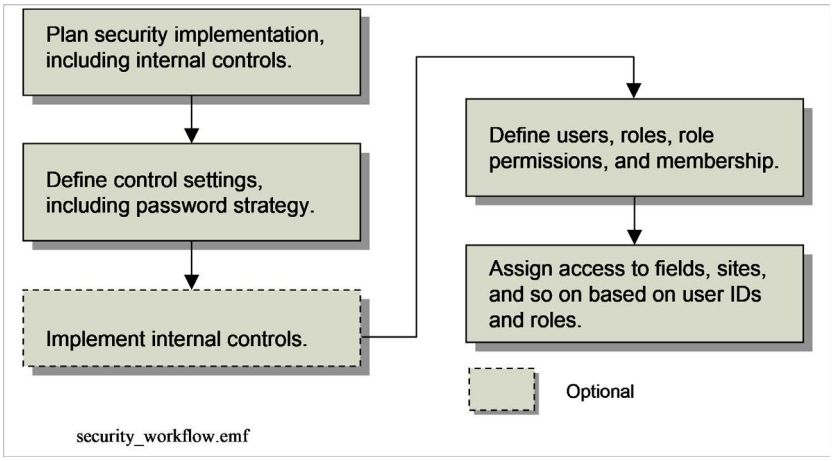
- Segregation of duties. Provides features that prevent a user from participating in more than two parts of a transaction or process. This is accomplished by partitioning the system application resources into mutually exclusive categories. See Chapter 8, "Segregation of Duties in Adaptive ERP," on page 149.
- 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 8, "Electronic Signatures in Adaptive ERP," on page 159.
- 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 the change, which program made the change, when the change was made, and what the change was. You can set up these functions for all tables or you can limit the audit trail recording activity to specific tables. See Chapter 10, “Auditing,” on page 211.

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 more information, see “System-Supplied Roles” on page 50.

Use the checklists provided in this section as a starting point of identifying key focus areas when deploying a security plan. For more information, see Table 1.1 on page 8.

You must 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 Segregation of Duties (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 Users 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. An important feature of this program is the Passwords frame, where you establish a system-wide password strategy. For more information, see page 29.
- 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. For more information, see page 45.
- 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. For more information, see page 131.

Security Planning Checklists

Tables 1.1 through 1.3 summarize various security controls that you must consider as part of an effective overall information security plan for the system. The relevance of each item depends on the 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 23
Optionally, determine and document any Segregation of Duties policy requirement. Also, describe how to divide application resources.	Setting Up Segregation of Duties
Document which users can access the system and which domains and entities they can access. This step will require an in-depth knowledge of your organization's security requirements.	• "Define Users" on page 60 • "Specify Access to Domains and Entities" on page 68
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 48
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 131
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, after they are used to access the system.	"Set Up Users" on page 58
Define policies and procedures to keep user and role information up to date.	
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 155
Determine procedures to be used to create new user accounts and communicate initial passwords (email, personal contact, other).	"Create a Password Strategy" on page 33
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 22
Define how often users are required to change passwords, and update the corresponding system security setting.	"Password Expiration Days" on page 35

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 29 • "Monitor System Security" on page 36
Define password policies and procedures, including password composition, length, expiration, and reuse of previous passwords.	"Create a Password Strategy" on page 33
Define policies requiring users to lock application sessions with a screen saver or similar tool when left unattended.	"Client-Level Security" on page 26

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 24
Consider blocking table and field access at the Progress level for the blank user ID.	"Progress Editor Access" on page 23
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 26
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 29
Define users assigned to the Security Administrator Role, who will receive email notifications of security events such as failed logins exceeding a defined threshold.	• "Email System" on page 31 • "Email System" on page 31
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 33

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 131
Review users and roles for potential segregation of duty issues and adjust assignments as appropriate.	Setting Up Segregation of Duties

Security and Internal Controls Menus

Table 1.4 lists the menus you use to define and maintain security and internal controls from QAD Adaptive.

Table 1.4
Security Features

Description	Resource URI
Role & Permissions	
Roles	urn:view:hybridbrowse:com.qad.qracore.roleV2s
Role Overview	urn:browse:mfg:mg115
Explicit Role Permissions Detail	urn:browse:mfg:mg046
Resource Identities	urn:browse:mfg:mg064
Resource Dependencies	urn:browse:mfg:mg047
Resource Mapping	urn:browse:mfg:mg052
Resource Mapping By Role	urn:browse:mfg:mg118
Explicit Role Permission Detail by App	urn:browse:bebrowse:com.qad.qracore.accessControlEntryApps
Permission Types	urn:browse:mfg:mg065
Resource Permission Types	urn:browse:mfg:mg100
Role Permission Sync	urn:browse:mfg:mg073
Role Permission Sync Detail	urn:browse:mfg:mg074
Role Resources Audit Report	urn:report:c1:QAD_RoleResourcesAudit
Field Security Patterns	urn:browse:mfg:mg082
Menus	
Menus	urn:view:hybridbrowse:com.qad.qracore.menuTreeV2s
Menu Details	urn:browse:mfg:mg049
System Menu Override	urn:browse:mfg:mg120
Role Menu Dependency	urn:browse:mfg:mg075
Application Menu Configuration	urn:view:maint:com.qad.qracore.applicationMenuConfiguration
Application Menu Configuration Details	urn:browse:bebrowse:com.qad.qracore.appMenus
Users & User Access	
Users	urn:view:hybridbrowse:com.qad.qracore.users2
User Access	urn:view:hybridbrowse:com.qad.qracore.userAccessLists
User Access Detail	urn:browse:fin:BUserRole.RoleMembership
Effective User Access Role Permissions Detail	urn:browse:mfg:mg061
User Access Audit Report	urn:report:c1:QAD_UserAccessAudit
User Monitor	urn:report:c1:QAD_UserMonitor
User Inquiry	urn:report:c1:QAD_UserInquiry
User Detail	urn:report:c1:QAD_UserAccountStatus
Domains	urn:view:hybridbrowse:com.qad.erp.base.domainV3s
Entities	urn:view:hybridbrowse:com.qad.erp.base.entityV3s
Sites	urn:view:hybridbrowse:com.qad.erp.base.sites

Description	Resource URI
Licenses	
Licensed Applications	urn:report:c1:QAD_Licensed_Application
License Violation	urn:report:c1:QAD_Detailed_License_Violation
Segregation of Duties	
SOD Categories	urn:view:hybridbrowse:com.qad.qracore.SODCategorys
SOD Category Membership	urn:view:maint:com.qad.qracore.SODCategoryMemberships
SOD Category Membership Detail	urn:browse:mfg:mg123
SOD Logs	urn:view:browse:com.qad.qracore.sodLogsBrowse
SOD Violations Rule 1	urn:browse:bebrowse:com.qad.qracore.SODViolation1s
SOD Violations Rule 2	urn:browse:bebrowse:com.qad.qracore.SODViolation2s
SOD Violations Report	urn:report:c1:QAD_SODViolationReport
SOD Role Permissions Comparison Report	urn:report:c1:QAD_SODRolePermissionsComparisonReport
SOD Control	urn:view:maint:com.qad.qracore.SODConfigurations
SOD Setup	urn:view:maint:com.qad.qracore.SODSetups
SOD Policy Exceptions	urn:view:hybridbrowse:com.qad.qracore.SODPolicyExceptions
SOD Policy Exceptions Details	urn:browse:bebrowse:com.qad.qracore.SODExceptionDetails
SOD Policy Exceptions Report	urn:report:c1:QAD_BLF_SODPolicyExceptionsReport
Record Security	
Record Level Security	urn:view:hybridbrowse:com.qad.qracore.resourceInstanceSecuritys
Security Rules	urn:view:hybridbrowse:com.qad.qracore.securityRule
Security Groups	urn:view:maint:com.qad.qracore.securityGroups
Secure Records	urn:view:browse:com.qad.qracore.secureRecordsBrowse
Secure Record Detail	urn:browse:mfg:mg084
E-Signature	
E-Signature Setup	urn:view:hybridbrowse:com.qad.qracore.ESignatureSetups
E-Signature History	urn:view:hybridbrowse:com.qad.qracore.ESignatureHistories
E-Signature History Detail	urn:view:hybridbrowse:com.qad.qracore.ESignatureHistoryLines
Other	
Apps	urn:view:hybridbrowse:com.qad.qracore.apps
My Developer Settings	urn:view:maint:com.qad.qracore.currentDeveloperSettings
Table: DataLoadFile	urn:browse:mfg:mg090
View Resource Metadata	urn:browse:mfg:mg048
Configuration Data	urn:view:hybridbrowse:com.qad.qracore.configurationDatas
Security Control	urn:view:maint:com.qad.qracore.securityControls
Logon Attempts	urn:browse:mfg:mg057
Logon History Archive/Delete	urn:report:c1:QAD_LogonHistory
Sessions	urn:view:hybridbrowse:com.qad.qracore.sessionMasters
Session Master	urn:browse:mfg:mg058
Client IDs	urn:view:hybridbrowse:com.qad.qracore.jwtClientV2s

Description	Resource URI
LDAP Instances	urn:view:hybridbrowse:com.qad.qracore.ldapInstanceV2s
Logging Options	urn:view:maint:com.qad.qracore.loggingOptions

Chapter 2

Security Overview

This chapter discusses the security features available in your system:

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 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 QAD Adaptive.

Roles

A role is a logical subset of activities that describes 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 and maintained by using Roles.

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 more information, see "Role Permissions".

Roles operate within the context of the domains and entities to which the user is granted access. This concept is known as role membership. For more information, see "Role Membership" on page 17. A user with multiple roles has access to all the resources assigned to each.

Role Permissions

Role permissions are defined by assigning a set of application resources to a role using Role Permissions in QAD Adaptive.

- For component-based functions, role permissions control the ability to use 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 of those. For more information, see "QAD Adaptive Security" on page 75.

The QAD Adaptive application resources defined in the system display in a tree layout. To define role permissions, you select the resources to assign to the role. Once role permissions and role membership are 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.

Role Membership

Role membership associates users and roles, as well as the domains and entities in which that role operates. Use User Access in QAD Adaptive 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 is generally relevant only within financial functions. Users who work 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 is assigned the role of 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 set up in Role Permissions limits who can update specific fields and field groups. For field security, specify a user ID.
- Update restrictions functions limit who can update specific records and create specific issue, receipt, and transfer transactions.
- GL Account Security Settings restricts access to GL accounts from operational functions. Specify any combination of user IDs or roles.

- Site Security limits who can create inventory transactions at secured sites. Specify any combination of user IDs or roles.
- Inventory Movements 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 more information about setting up operational programs, see “Additional Security for Standard Programs” on page 131.

Additional Security for QAD Adaptive

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

- 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 QAD Adaptive are determined by role security.

For details on setting QAD Adaptive security, see “QAD Adaptive Security” on page 75.

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 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 more information, see “Create a Password Strategy” on page 33.

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, Users lets system administrators force an individual user to change the password at next sign in. Force Password Change checkbox on the Change Password panel of Users makes all users or specified roles change their passwords. For more information, see “Update Passwords” on page 66.

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. For more information, see “OS-Based Sign-in Security” on page 22.

  Note You also should consider additional access security options at the operating-system and Progress levels. For more information, see “Operating System and Progress Security” on page 23 .
- Domain/entity security limits individual user access to the domains and entities identified in User Access. 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 interdependent, working together to ensure users can access only the business areas for which they are 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. The system next checks if the user has access to any domains and entities defined in User Access.

Note To sign in to the QAD Adaptive, a user must be assigned the **webui_user** role. In addition, the user must have access to at least one site and a default domain must be selected.

To change domains in QAD Adaptive, 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.

At no time can a user access an entity that is not authorized in their user record. For more information, see “Specify Access to Domains and Entities” on page 68.

For details about using and managing workspaces, see *Introduction to QAD Adaptive Applications User Guide*.

Sign-In and Security Control

Use Security Control to define additional security measures related to system sign-in.

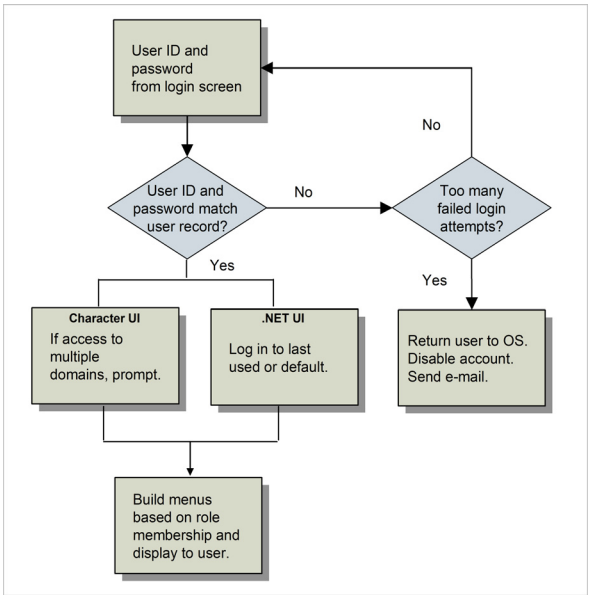
If a user enters an invalid combination of user ID and password, the system may prompt additional times—based on the value of Maximum Access Failures in Security Control. After the specified number of failures, the user is returned to the operating system, the user account is disabled, and system administrators 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 this process.

You can configure the system to use the operating system user ID to grant access, thereby completely or partially bypassing the standard sign-in process. For more information, see “OS-Based Sign-in Security” on page 22.

Depending on the setting specified in Security Control, the system maintains historical records of successful and failed sign-in attempts. Use Logon Attempts to view the 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 Base Control.

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. For more information, see “OS-Based Sign-in Security” on page 22.
- 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.

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.

QAD Adaptive supports 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 to QAD Adaptive 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 Users.

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. The default minimum password length is 12 characters.

Operating System and Progress Security

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, you can use operating system commands (such as the following in UNIX) to limit both Read and Write permissions 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 accesses 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, assign appropriate access permissions to the roles you want to be able to access Progress Editor, and then assign these roles to legitimate Progress Editor users.

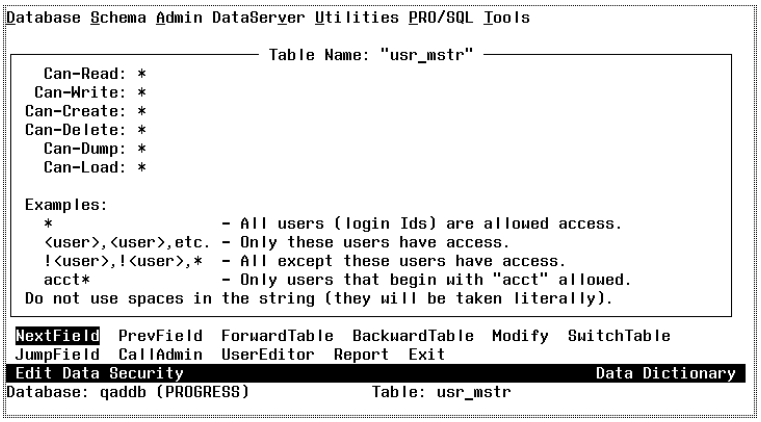
Another related control that should be considered is to block privileges for users connecting to the application database with a blank user ID. The Disallow Blank User ID Access option on the Progress Database|Admin|Security menu is available for this purpose. For more information, see the “Maintaining 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 mark (!) 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. For more information, 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 lets you specify the number of minutes of inactivity that can occur before the system automatically signs a user out of an application session. Designed primarily to reduce system load caused by inactive users who remain signed in unnecessarily, this feature also strengthens 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. For more information, see “Idle Timeout Minutes” on page 30.

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

Client Security

If you need to configure the Apache reverse proxy on-premise (not recommended), you must define the Content Security Policy (CSP) and Permission Policy headers.

- **Content-Security-Policy (CSP):** A response header that specifies which resources a web page is allowed to load. Proper configuration helps mitigate risks such as Cross-Site Scripting (XSS), Clickjacking, and other code or data injection attacks.
- **Permissions-Policy:** A response header (formerly known as Feature Policy) that specifies which browser features and APIs can be used. It also controls which origins can access these features, both on the top-level page and in embedded `iframes`.

QAD Adaptive Security

The QAD Adaptive 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 chapter discusses how to set up basic security in your system.

Define General Security Settings

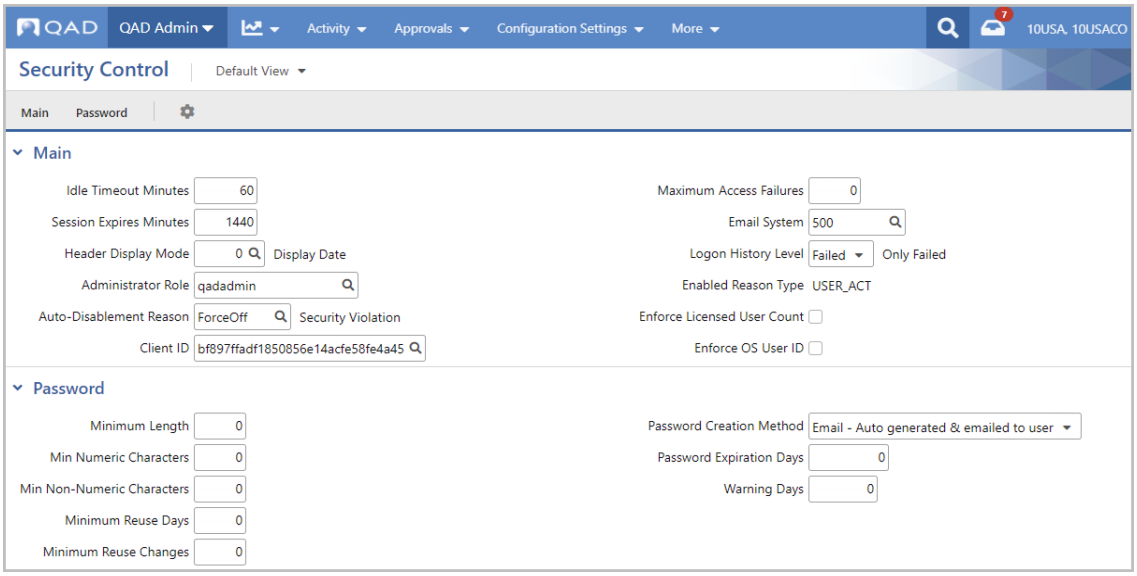
In QAD Adaptive, you can configure security settings through the Security Control screen. From this interface, you can perform the following functions:

- Establish the 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 through this screen:

- Each time a field is updated, the system notifies administrators by e-mail. For more information, see “Set Up Email Notifications” on page 35.
- You must use this program to update data values in the user control (usrc_ctrl) table. The system prevents you from using other methods, such as Progress Editor, to modify that record.

Fig. 3.1
Security Control



Main Panel

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. The default value is 60.

Note If a nonzero value is entered in this field, the Timeout daemon must also be configured and started. For more information about daemons, see *QAD System Administration User Guide*.

The field can also be used as part of an overall security strategy to prevent users from inadvertently allowing access to unauthorized individuals. For more information, see “Client-Level Security” on page 26.

Note This setting does not affect QAD Adaptive. QAD Adaptive 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.

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

- 0 — Display Date
- 1 — Display User ID
- 2 — Display Date and Domain
- 3 — Display User ID with Domain

Note The setting is not applicable for QAD Adaptive.

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.
- If you use 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. For more information, see page 35.

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

Auto-Disablement Reason. Specify the reason code the system enters in user records when it automatically disables a user account. This occurs when a user reaches the number of consecutive failed sign-in attempts specified in Maximum Access Failures. This code must be defined in Reason Codes 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 IDs.

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. You can specify any value from 1 to 20. The default field value is 10. For more information, see "Set Up Email Notifications" on page 35.

Note If you use electronic signatures, this value controls the number of failed signature attempts that are allowed before the system disables the user ID.

Email System. Specify an email system definition 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 Users. 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. For more information, see “Monitor System Security” on page 36.

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 read-only field. The system-assigned value is USER_ACT, the reason type associated in Reason Codes 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 Users. For more information, see “Enabled Reason” on page 66.

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

- AUTO. The system automatically disables the account. You can enter this in Auto-Disablement Reason.
- REACT. The system administrator manually re-enables the account.
- NEW. The system administrator adds an account for a new user.
- LEFT. The user is no longer with the organization, and the system administrator disables 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, the existing user records are populated with this value. After you set up values in Reason Codes that apply to your system, you do not have to use this default reason code.

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 Users, when you attempt to add users or assign them 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 if the system allows users to access character sessions for the application based on their operating system sign-in. For more information, see “OS-Based Sign-in Security” on page 22.

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.

Create a Password Strategy

Use the Password panel 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 use 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 on the Main panel 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. For more information, see “OS-Based Sign-in Security” on page 22.

Password Panel

Minimum Length. Enter the minimum number of characters allowed for new passwords. Password cannot exceed 16 characters.The field default value is 12.

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 the Force Password Change checkbox on the Change Password panel of Users to force users change their passwords at the next sign-in. New passwords must meet the updated structure requirements. For more information, see “Monitor System Security” on page 36.

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 less 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 changes 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 more information about password maintenance, see “Update Passwords” on page 66.

- 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 Users. The system administrator must then communicate it to the user.
- Email. A temporary password is automatically generated and e-mailed to the email address defined in Users 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. For more information, see “Set Up Email Notifications” on page 35.

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.

Password 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 Users, the Change Password panel. The date is printed in Universal Time, Coordinated (UTC). For more information about the time stamping of transactions outside domains, see *QAD System Administration User Guide*.

Warning Days. Specify the number of days before a password expires 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 Users, the Change Password panel.

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 the 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 on the Password panel of Security Control, the system generates a new password and emails it to the user based on the email address specified in Users. This occurs for new and existing users when the Force Password Change checkbox is selected in Users. 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 reenables it.
- When an account is disabled, the email system can automatically notify system users that are assigned the 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. The Force Password Change checkbox on the Change Password panel of Users lets the administrator force users to update their passwords based on role, domain, and/or the date of the last change.

  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 Users 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

Authentication

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

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.

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 QAD Adaptive.
- 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 the `configuration.properties` file with SAML SSO examples on page 42.

Define the properties described in Table 4.1 to enable and configure SAML SSO.

Table 4.1
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
qad-webshell.saml.jwt.clientSecret	The client secret. See “Client ID and Client Secret”	qad-webshell.saml.jwt.clientSecret= zsSMtrHLMFDxG3dhEc3lTtXIyGvPBEhPn46wraCPLP8=
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>
```

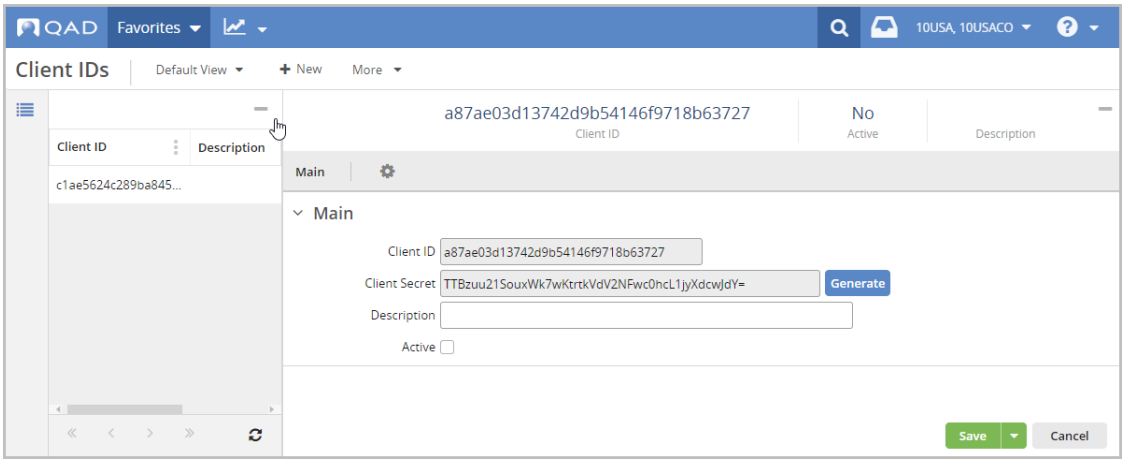
Client ID and Client Secret

The client ID and client secret settings can be created in QAD Adaptive.

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 IDs in the QAD Adaptive. Select New.
2. Select Generate to create a new client ID and client secret.

Fig. 4.1
Client IDs



3 Enter a description of the generated client ID and select the Active checkbox. Click Save.

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 `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 4.2 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
```

Chapter 5

Users and Roles

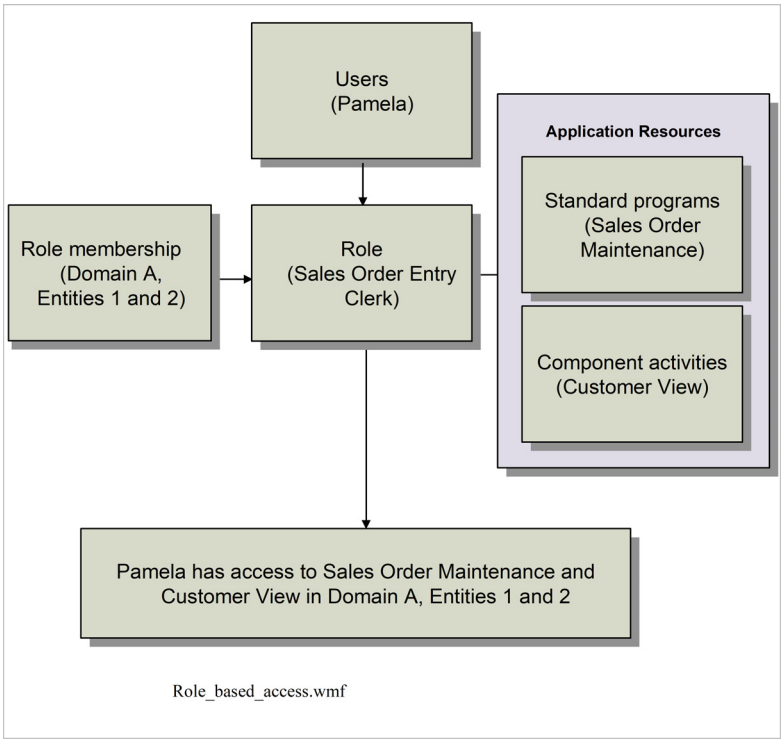
This chapter describes how to set up users and roles in your system.

Overview

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

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

Fig. 5.1
Users and Roles

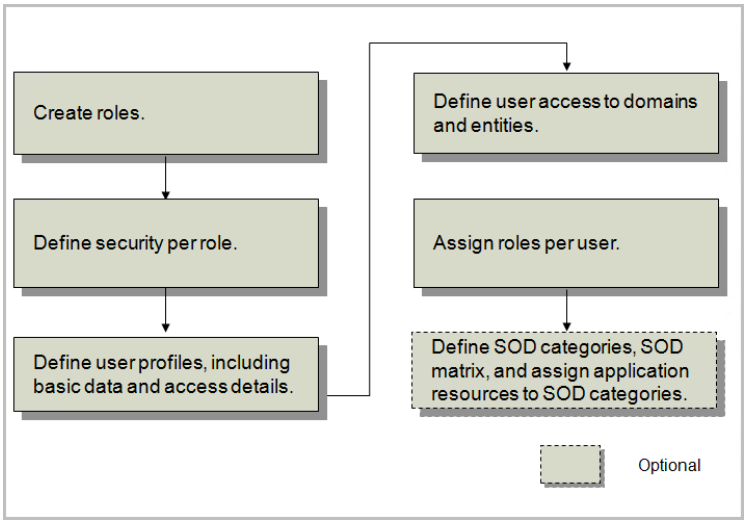


Role and User Definition Process Workflow

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

To set up and configure users and roles in your system, use the Roles and Users screens in QAD Adaptive. Figure 5.2 shows the user and role setup process workflow.

Fig. 5.2
Roles and Users Setup Flow



Follow the steps in the workflow below to set up users and roles:

1. Create roles using Roles in QAD Adaptive. All system users must be assigned to a role before they can access the system. For details, see “Set Up Roles” on page 48.
2. After creating user roles, define role permissions using Role Permissions. 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 58.
3. Create system users in Users, 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 58.
4. Specify user access to domains and entities in User Access. For details, see “Specify Access to Domains and Entities” on page 68.
5. Then use User Access to assign users to roles and specify the role context—that is, how the role operates within domains and entities. For details, see “Define Role Membership” on page 70.
6. 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 are defined, role permission definitions are constrained by your segregation of duties policy. Implementing segregation of duties is optional. See Chapter 7, “Segregation of Duties in QAD Adaptive,” on page 121.

Set Up Roles

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

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

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

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

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

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

Uses of Roles

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

- Limit access to other resources such as sites and GL accounts. This is described in Chapter 7, "QAD Adaptive ERP Security," on page 123.
- 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 Process Maps are available under the Help menu icon in QAD Adaptive, 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 User Access. 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.

QAD Adaptive 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 Permissions 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 QAD Adaptive role based on a default or existing role, see "Role Menus" on page 78 for information on copying menu items and setting permissions.

System-Supplied Roles

During system installation, a number of roles are set up automatically in QAD Adaptive. Table 5.1 lists these roles and their functions.

Table 5.1
System Roles Created During Installatio

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 Customers so that the operational data can be completed.
EmployeeNotify	Members of this role receive email notification when a new employee record is created with Employees so that the employee can be defined as a service/support engineer in Engineers.
EndUserNotify	Members of this role receive email notification when a new end user record is created with End Users so that the operational data can be completed.
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 Suppliers so that the operational data can be completed.

The SuperUser role is initially defined to provide permissions for all menu functions loaded in the system. 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 59.

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

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

Role Example

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

The system administrator creates three roles: *Clerk*, *Manager*, and *CFO*. Sara, the AP Clerk, is assigned to the Clerk role. Don, the AP Manager, is assigned to the Manager and Clerk roles. Jane, the CFO, is assigned all three roles. In this setup, illustrated in Figure 5.3, Jane’s roles grant her entry to all the levels she is authorized to access.

Fig. 5.3
Using Roles to Give Access

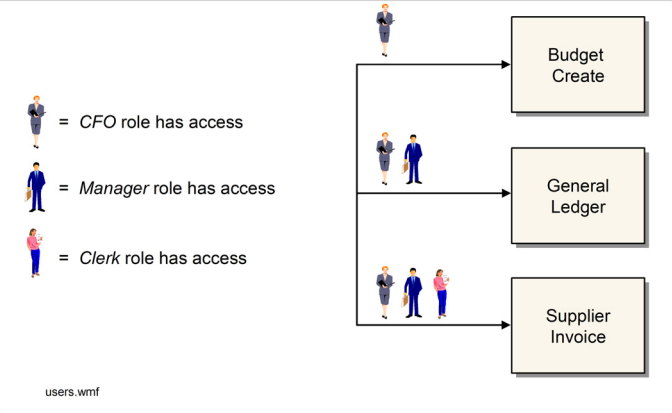


Table 5.2 shows how the system administrator assigns users to each role.

Table 5.2
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, users can also create their own custom menu display under Favorites.

Define Roles

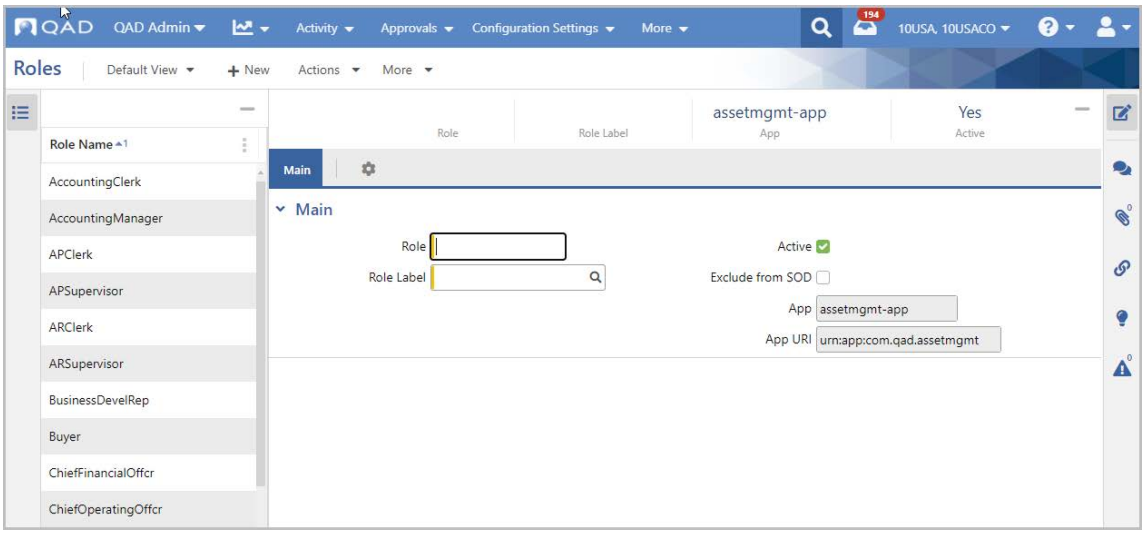
In QAD Adaptive, use Roles to define roles in your system. You should define as many roles as required in order to model your business processes in the system. This screen also allows you to view and perform maintenance on existing roles.

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 QAD Adaptive Role

1 Select New.

Fig. 5.4
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 to exclude this role 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.

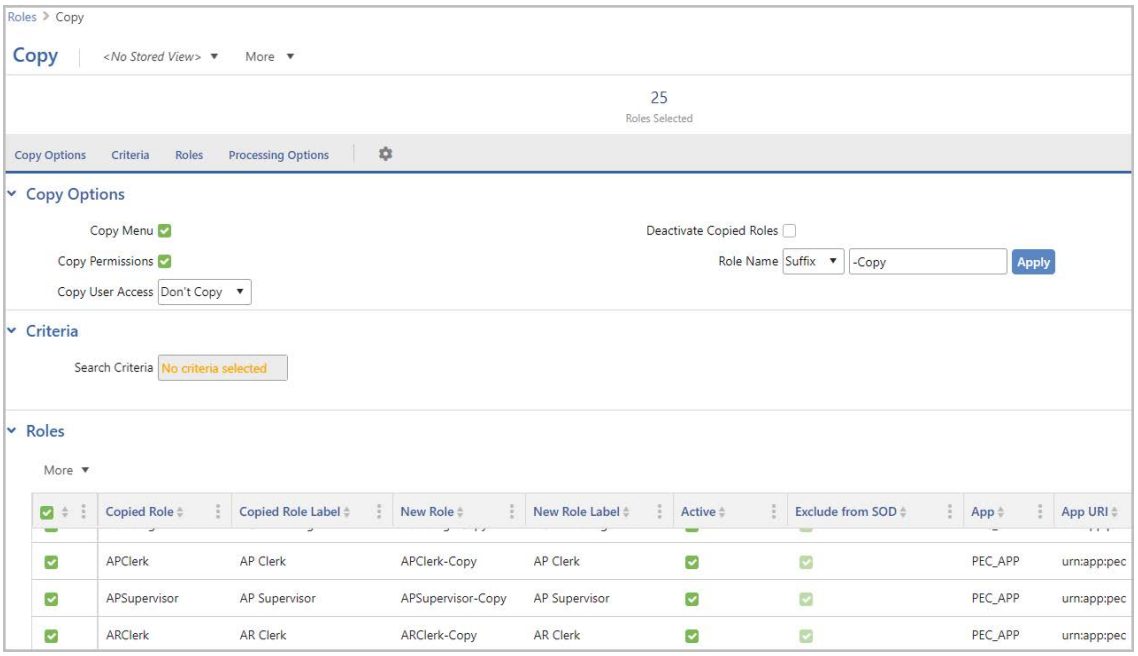
8 Assign permissions to the new role through role menus. See “Role Menus” on page 78.

Copy a QAD Adaptive Role

The Copy action in Roles lets you copy role's permissions, and, optionally, copy the users assigned to the role and assign them to the new role. You have an option not to copy user assignments, replicate user assignments from the copied role to the new role, or move 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. 5.5
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' permissions.

Copy User Access. Select one of the following options to indicate how you want to treat users assigned to the copied roles:

- 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 You cannot replace user access for the following roles: SuperUser, QADAdmin, WebUI_User, admin role set in Security Control, and 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 54.

Select one of the following options:

- 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

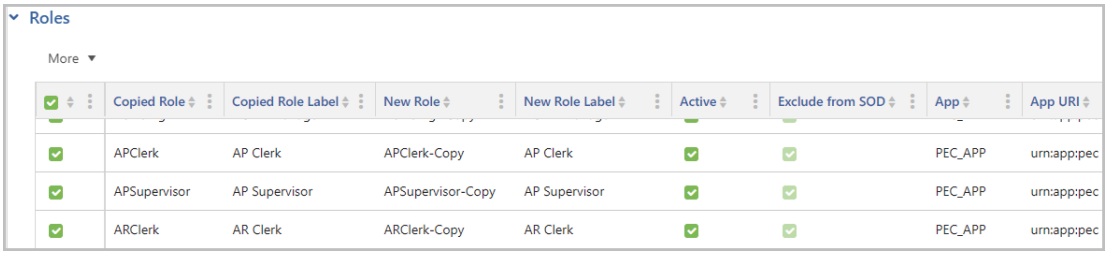
Search Criteria. This field displays the search criteria passed from the browse.

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. 5.6
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, 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

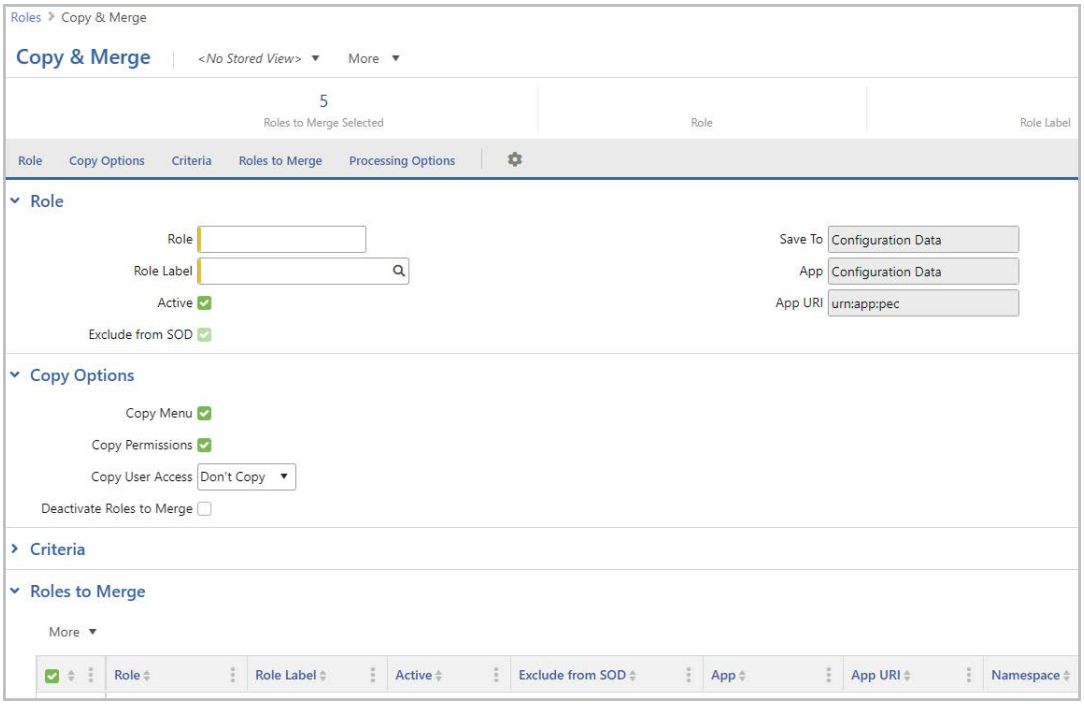
The Processing Options panel includes one field, Process in Background, which is always selected and read-only. When you configure your role copy options, click **Submit** to submit the copy action for processing. The system displays a message to indicate that the results will be sent to your inbox.

Copy and Merge QAD Adaptive Roles

The Copy & Merge bulk action lets you copy the menus, permissions, and user access from multiple roles and 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. 5.7
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 54, “Roles Panel” on page 54, and “Processing Options Panel” on page 55.

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 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 one of the following options to indicate how you want to treat users assigned to the copied and merged roles:

- 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 You cannot replace user access for the following roles: SuperUser, QADAdmin, WebUI_User, admin role set in Security Control, and roles that have no App URI.

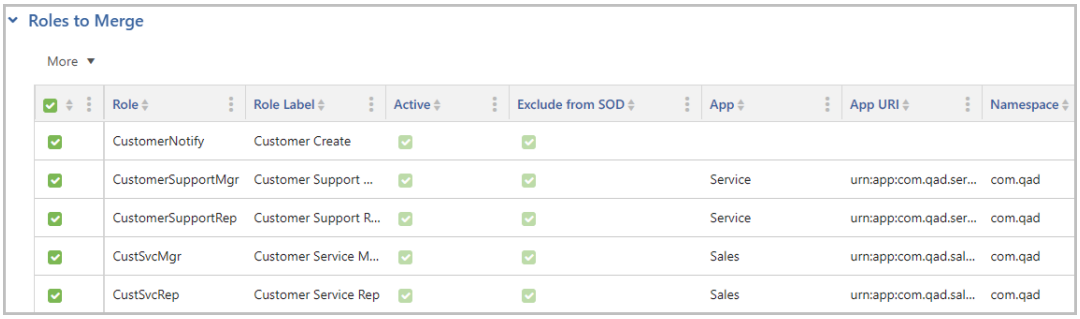
Deactivate Roles to Merge. Select this field to deactivate the roles to merge. This field is cleared by default.

Note You cannot deactivate the following roles: SuperUser, QADAdmin, WebUI_User, admin role set in Security Control, and 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. 5.8
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 54.

Define Role Permissions

Use Role Permissions 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 In QAD Adaptive, permissions can be defined in three places:

- On the Role Permissions page
- Under Menus > Role Menu or Favorite (User) Menu > Permissions
- Through Contextual Permissions (accessible from any page via More > Permissions)

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 resources 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.
- 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.
- 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.

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

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 Users in QAD Adaptive, 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 multiple QAD applications with Directory Services, such as Active Directory or Open LDAP.

With user synchronization, QAD Adaptive 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 and a corporate LDAP directory.

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.

Once users are synchronized, continue setting up users with “Specify Access to Domains and Entities” on page 68.

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.

- Base Control 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 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

Access Users in QAD Adaptive to assign a unique ID to a system user and define related application and security details.

To access the system, each user must specify a unique user ID and the associated password. In addition each user must be 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.

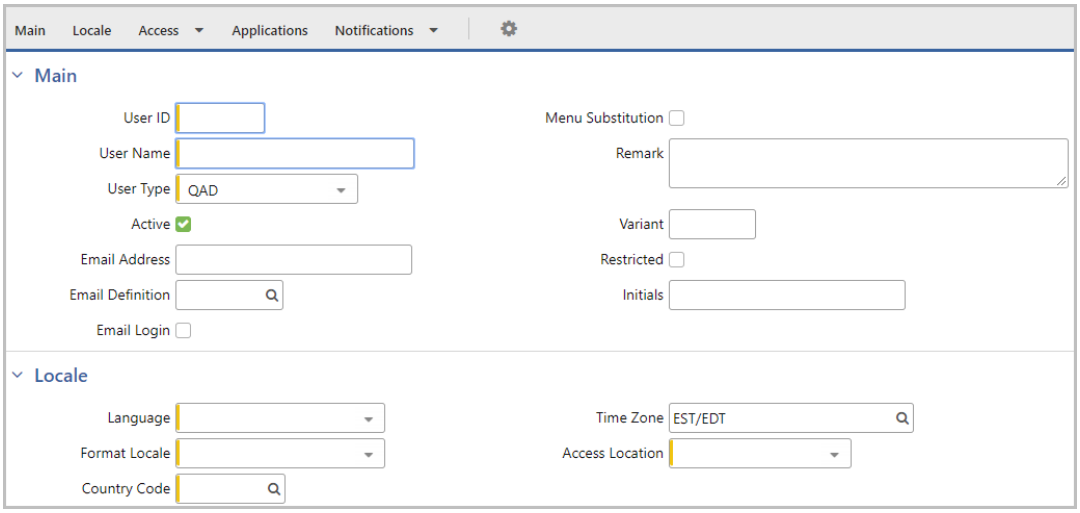
Once a user access the system, the ID cannot be deleted. Instead, you can deactivate a user's record in the system. If an ID has never been used for sign in, you can delete it, if necessary. This lets you correct any errors made during initial setup. This restriction ensures a complete audit trail of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

Important The Active checkbox and the System Access Enabled checkbox in Users 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 System Access Enabled checkbox determines whether a user can sign in. By default, the checkbox is selected when a new user is created. A user can sign in to the system only if both the System Access 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 Users are time stamped in Universal Time, Coordinated (UTC). For more information on the time stamping of transactions outside domains, see *QAD System Administration User Guide*.

Fig. 5.9
QAD Adaptive 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 (/ \). It is not recommended 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 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 22.

Depending on the setting of Header Display Mode in Security Control, the system may display this value on every program screen in the character interface. In the QAD Adaptive, the user ID always displays in the bottom message area. See “Email System” on page 31.

User Name. Enter a user name (maximum 35 characters) identifying the full user name associated with this ID. User name must only contain alphanumeric characters, space, and the following symbols: -,.~' .

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.

Variant. Optionally enter the locale for the user. This field can be used to specify regional variations within a country.

Define Basic User Information

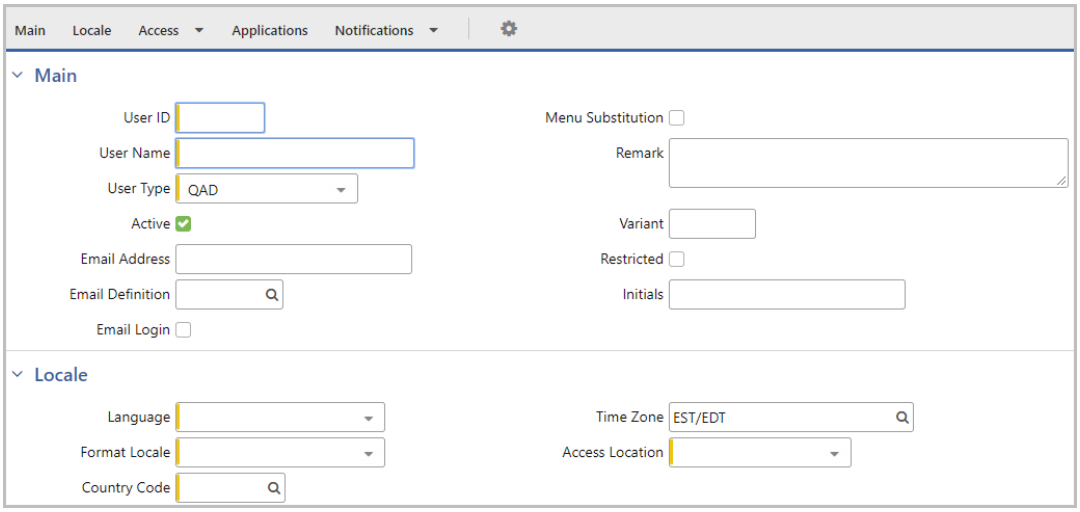
Defining basic information about system users includes setting options and defining values for:

- 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 Users.

Fig. 5.10
QAD Adaptive 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 are not 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 Countries. The country code also must have an associated alternate country code.

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.

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:

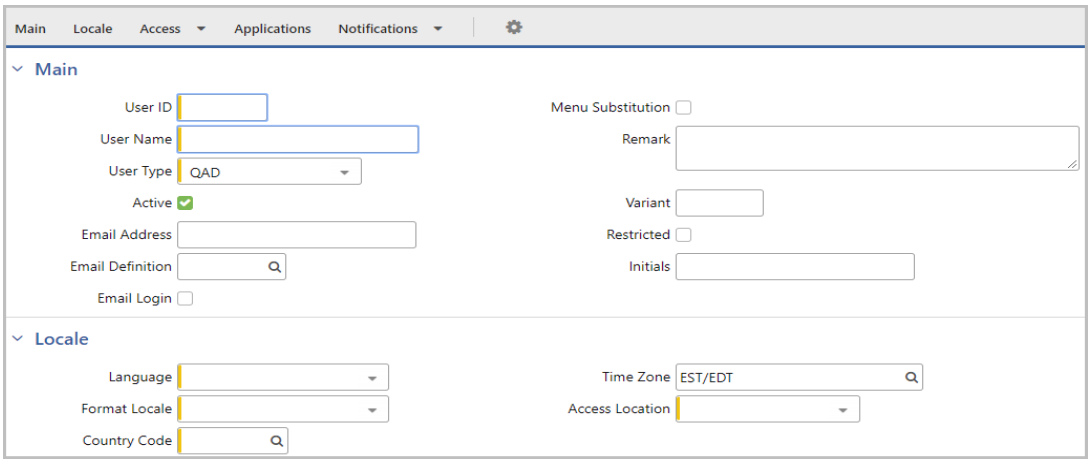
```
US,en,US,,mdy,American
```

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. 5.11
QAD Adaptive 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 Users.
- QAD identifies QAD employees who provide 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 Details 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.

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 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 is 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 and the ID is disabled.

Specify Email Addresses

Associate a valid email address and definition with each user who receives system-generated messages by entering values into the Email Address and Email Definition fields. When selected, the Email 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 Active Directory Access

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

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

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

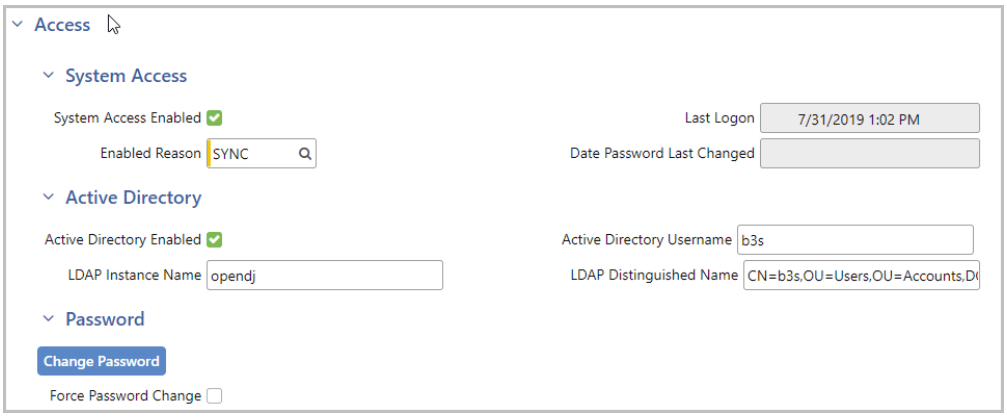
Active Directory Username. Enter the Active Directory username for this user. This username is limited to 64 characters.

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 Access panel in Users to specify security-related access settings for each user.

Fig. 5.12
QAD Adaptive Users (Access Panel)



System Access 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 System Access Enabled checkbox has a different function than the Active checkbox. The System Access 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.

The System Access Enabled field is updated in the following ways:

- Automatically when you enter a new user ID. By default, the system selects the System Access 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 “Email System” on page 31.
- 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 System Access Enabled. This reason code must be associated with reason type USER_ACT. See “Create a Password Strategy” on page 33.

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

Force Password Change. Indicate whether the system should force this user to create and validate a new password the next time they sign 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.

Select Force Password Change checkbox on the Change Password panel of Users for users belonging to selected roles.

Note Any updates made using the Force Password Change checkbox 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.

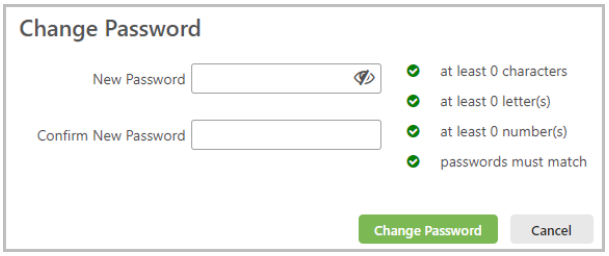
Update Passwords

When you click the Change Password button on the Access panel, 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 Users are single-use, temporary passwords generated by the system or entered by the system administrator. At sign in, the user is prompted to enter a new password.

Fig. 5.13
QAD Adaptive 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. To change password, click the Change Password button on the Change Password panel. See “Password Expiration Days” on page 35.

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 32.

- 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.

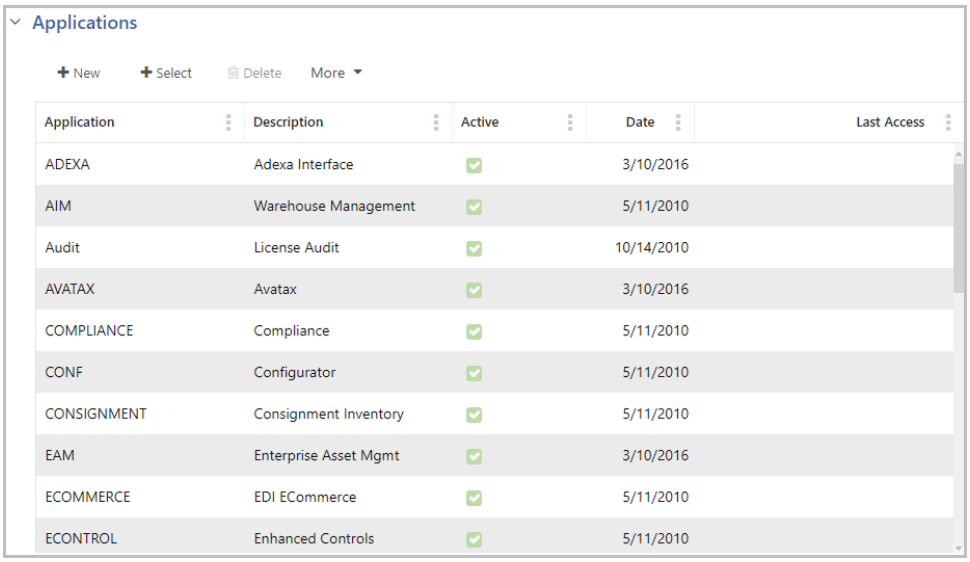
The applications that a user can access must be activated for the user; otherwise, the user cannot access the application. You can activate access to applications here.

Once a user accesses 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 Applications panel in Users 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. 5.14
QAD Adaptive, Applications Panel



The application name you enter under Application Name must be registered with the system. 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.

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

Specify Access to Domains and Entities

To create or maintain user access privileges for domains and entities, use User Access in QAD Adaptive. 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.

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 and Pending Invoices, 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 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 Access. You must explicitly grant users access before any updates can be made in the new domain.

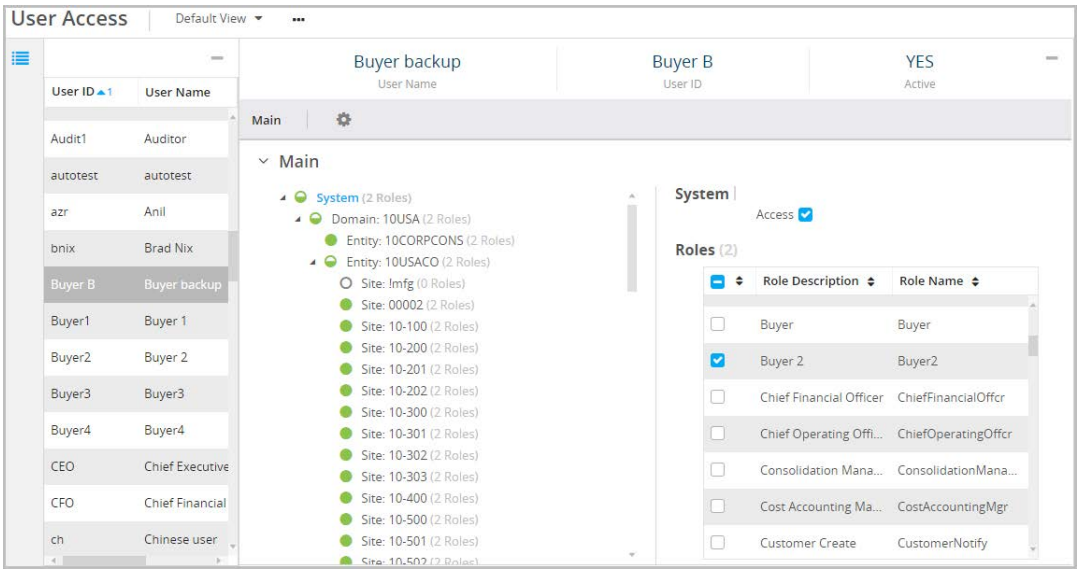
Any changes to user's domain or entity access privileges automatically update that user's role membership information. For example, removing user's ability to access an entity breaks the association between that entity and the user's assigned role, and the entity is deleted from the list of assigned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

Assign Access in QAD Adaptive

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 QAD Adaptive user must be assigned at least two roles, one of which is webui_user. A user cannot access QAD Adaptive without the webui_user role.

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. 5.15
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 Site Security.

The System tree is a hierarchical view of all domains, entities, and sites within QAD Adaptive. 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 5.15, 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.

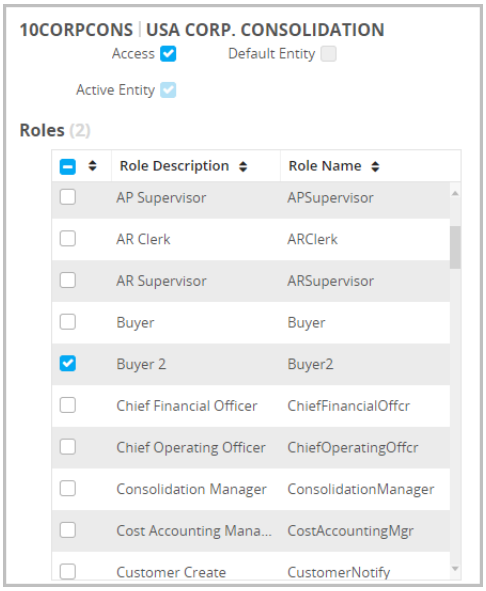
Define Role Membership

Use User Access in the QAD Adaptive 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 49 for details.

QAD Adaptive User Access Roles Grid

The Roles grid on User Access displays all of the roles in QAD Adaptive. 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. 5.16
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.

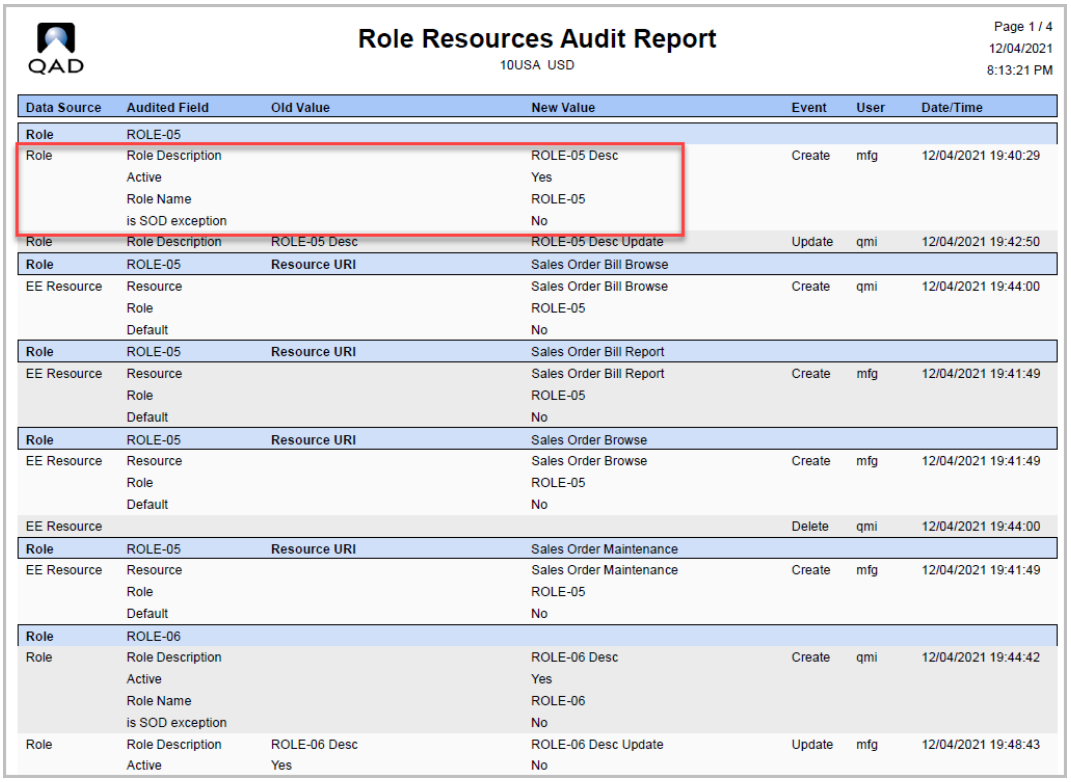
Figure 5.16 shows the roles in entity 10CORPCONS. You can modify role assignments for the selected user using the Roles grid.

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 role permissions.

Fig. 5.17
Role Resource Audit Report



QAD

Role Resources Audit Report

10USA USD

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

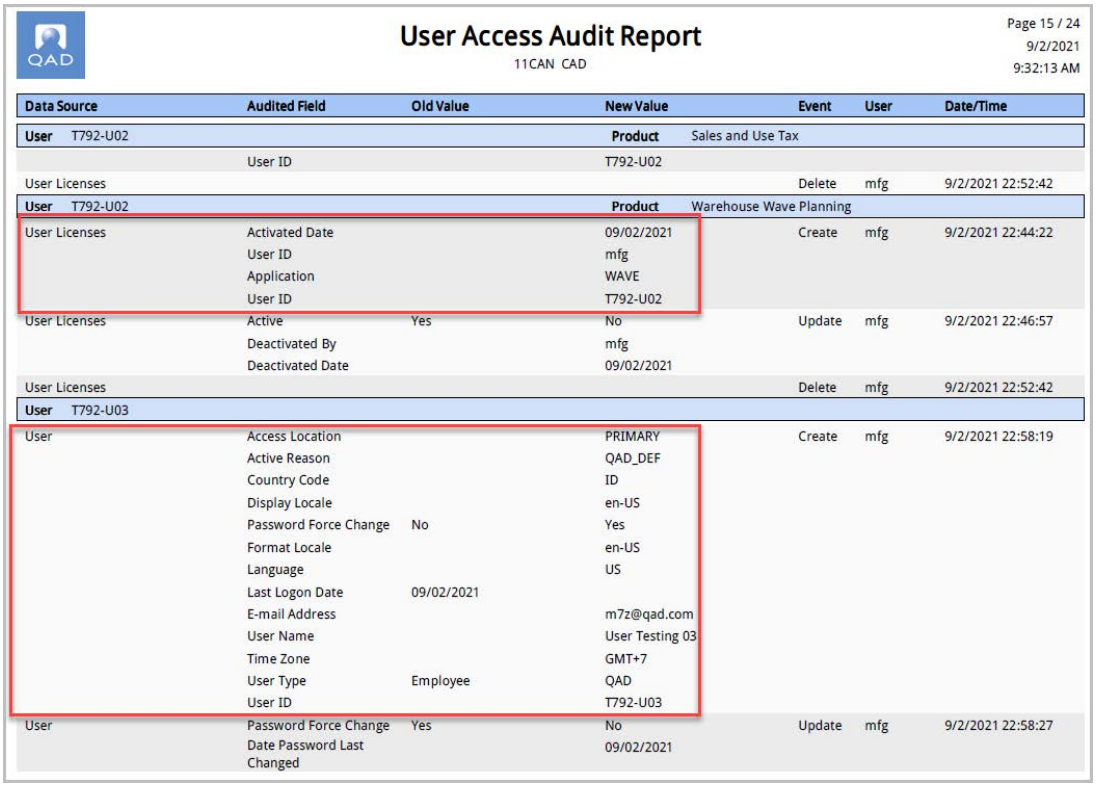
Data Source	Audited Field	Old Value	New Value	Event	User	Date/Time
Role	ROLE-05					
Role	Role Description		ROLE-05 Desc	Create	mfg	12/04/2021 19:40:29
	Active		Yes			
	Role Name		ROLE-05			
	is SOD exception		No			
Role	Role Description	ROLE-05 Desc	ROLE-05 Desc Update	Update	qmi	12/04/2021 19:42:50
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 5.17, 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. 5.18
User Access Audit Report - Example 1



User Access Audit Report
11CAN CAD

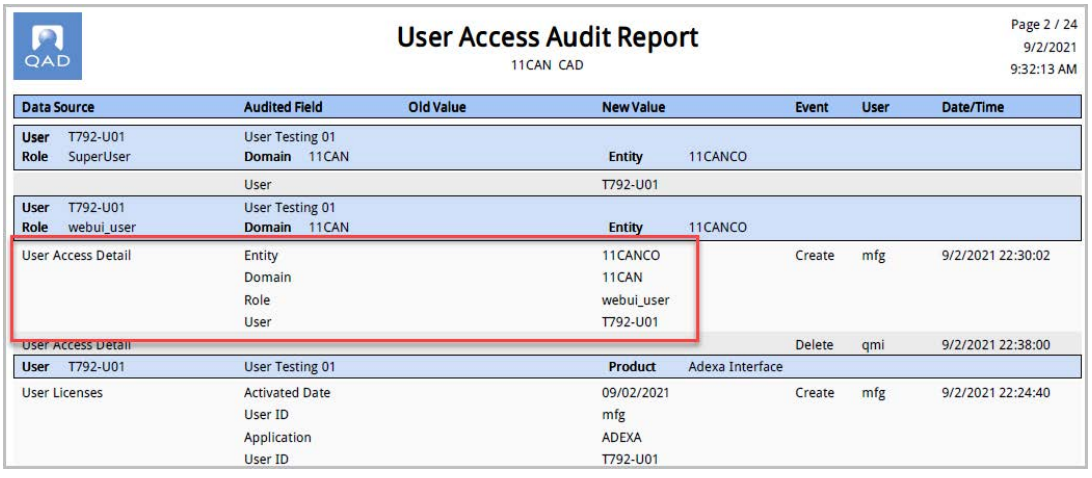
Page 15 / 24
9/2/2021
9:32:13 AM

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 5.18 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. 5.19
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 5.19.

For more detailed information on audit trail reports and enabling auditing in your environment, see Chapter 10, “Auditing,” on page 211.

Chapter 6

QAD Adaptive Security

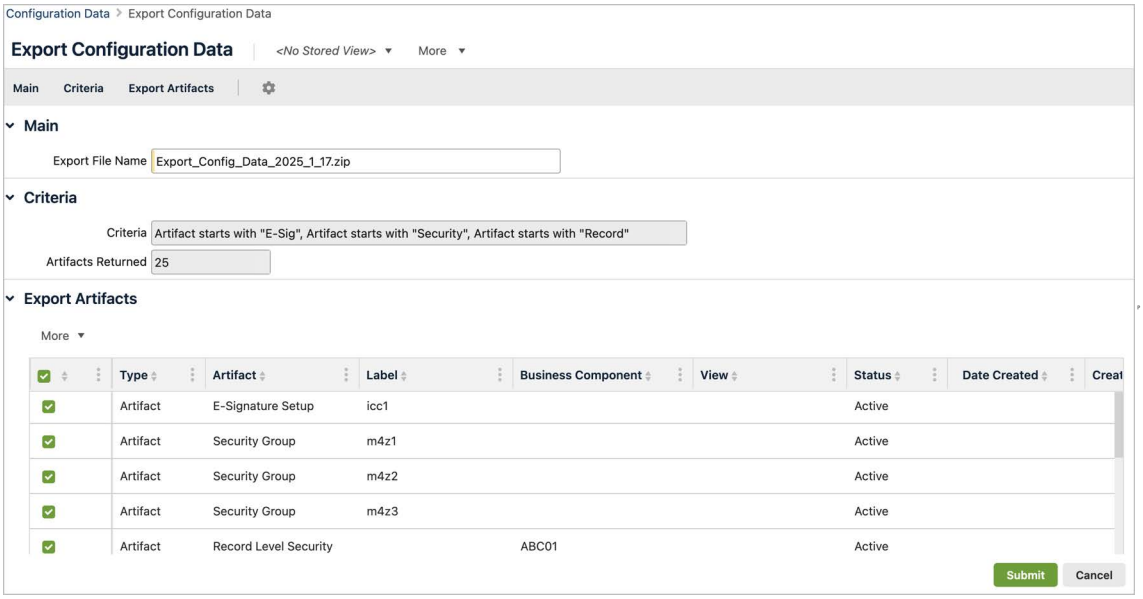
This chapter covers the following QAD Adaptive Security topics:

Prerequisites

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

You can export and import security configurations—including eSignature, Application Menu Configuration, Record Level Security for Security Groups and Security Rules—through the Configuration Data screen, as shown in Figure 6.1. This feature enables you to transfer configurations across different environments.

Fig. 6.1
Export Configuration Data



Role and User Workflow in QAD Adaptive

1. Create roles. See “Set Up Roles” on page 48.
2. Create role menus for the newly created roles and assign permissions to those role menus. See “Role Menus” on page 78.
3. Create system users. See “Set Up Users” on page 58.
4. Specify user access to domains, entities, and sites in User Access. See “Assign Access in QAD Adaptive” on page 69.
5. Assign users to roles in User Access. All QAD Adaptive users must be assigned to at least two roles, one of which is webui_user, before they can access the system. See “QAD Adaptive User Access Roles Grid” on page 70.
6. Configure settings for stored views, which allow users to customize screen layout. See “Configure Stored Views Access” on page 104.

Resources

QAD Adaptive 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.

Resources in QAD Adaptive range from the app level down to individual fields.

QAD Adaptive Resources

The following resources can be secured in QAD Adaptive.

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 QAD Adaptive.

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 QAD Adaptive 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 QAD Adaptive.

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

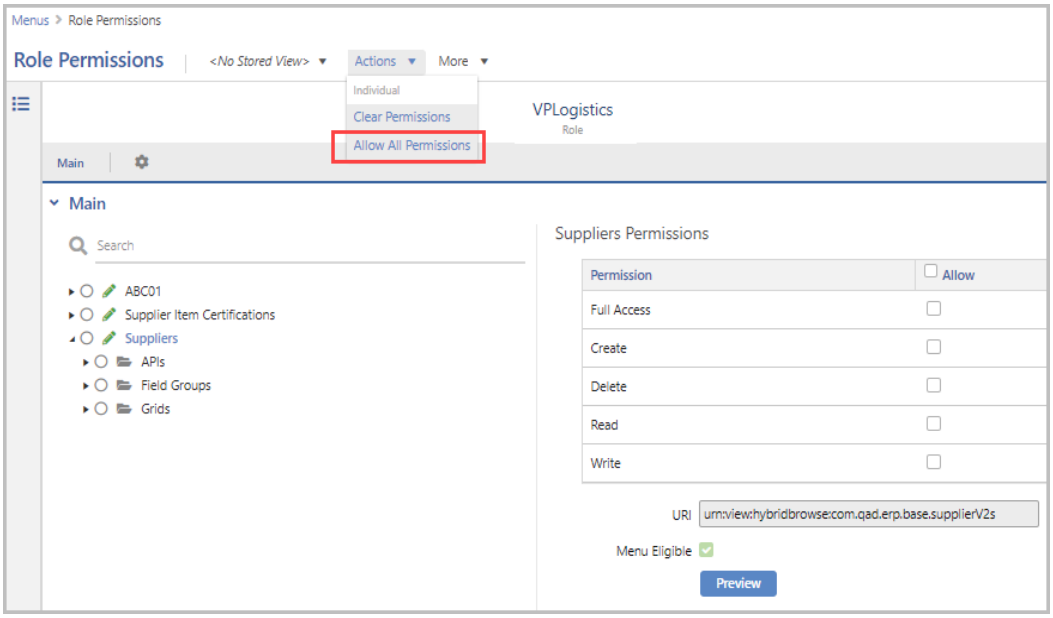
Create a New Role Menu

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 QAD Adaptive Role” on page 52.

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 QAD Adaptive.

Fig. 6.2
Allow All Permissions



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

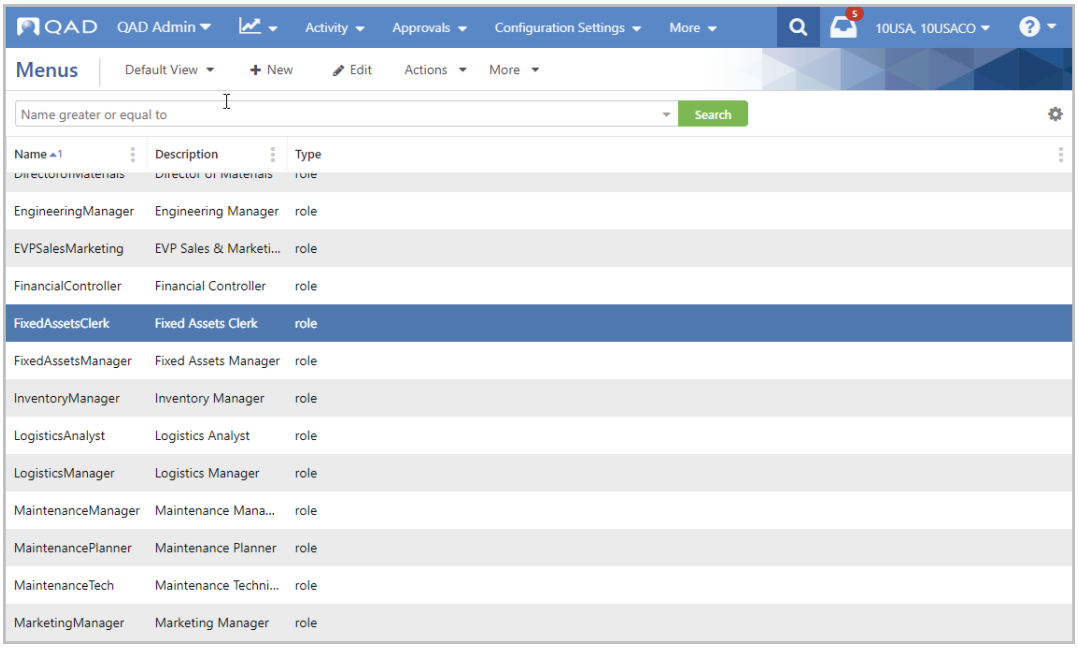
9 All of the secured resources should now have a green circle next to them. The system saves the setup automatically.

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 QAD Adaptive Role” on page 52.

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

Fig. 6.3
Menus

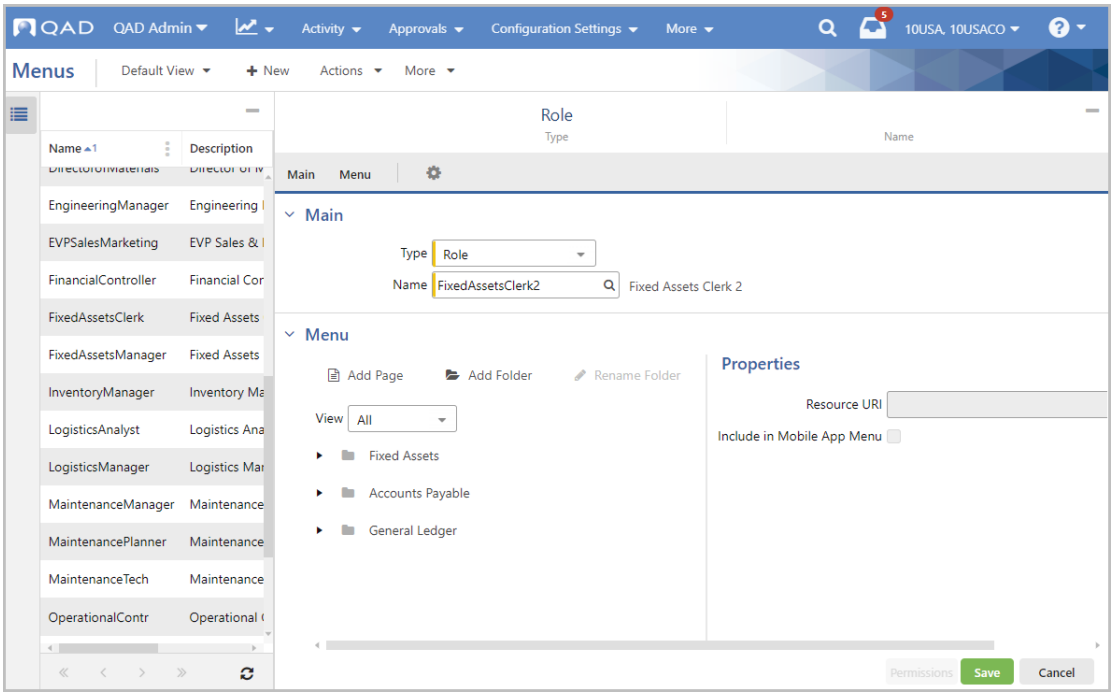


2 Select Copy from the Actions menu.

3 Select Role from the Type drop-down menu.

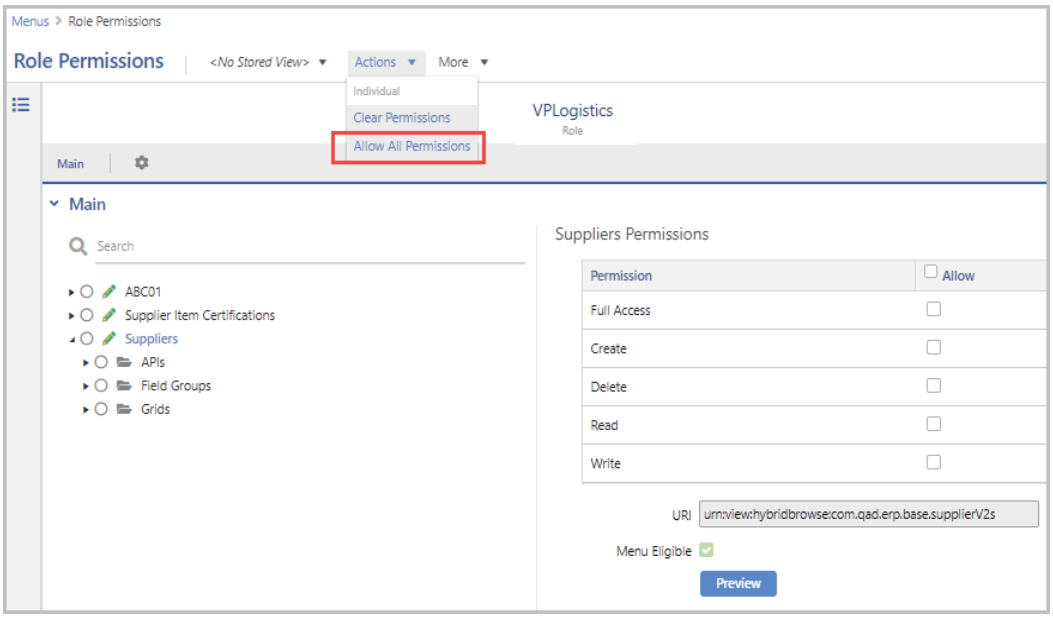
4 In the Name lookup, select the role that will be assigned this role menu.

Fig. 6.4
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 QAD Adaptive.

Fig. 6.5
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 QAD Adaptive. 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.

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.

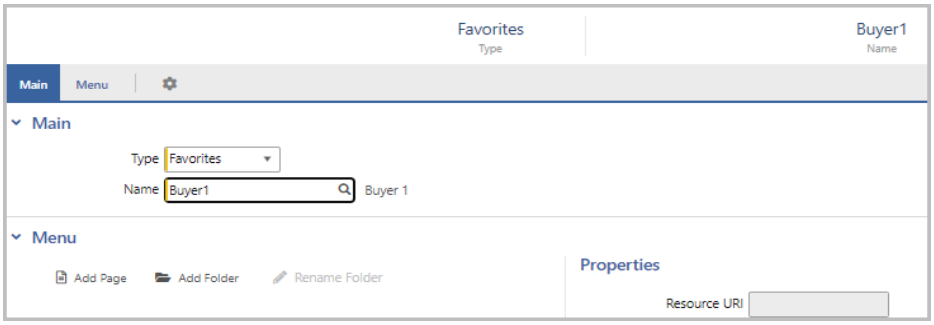
Create a New Favorites Menu for a User

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. 6.6
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**.

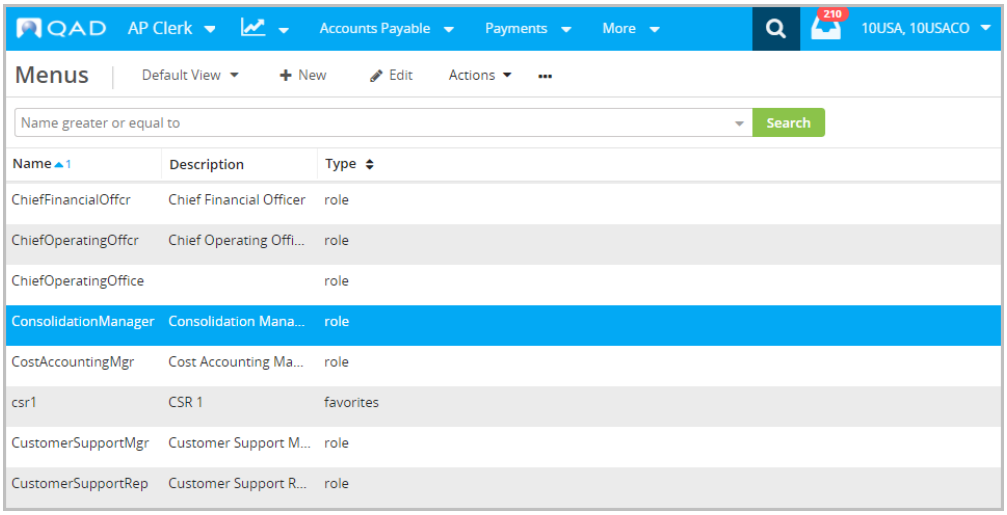
6 Click **Permissions** to check that the user's role has adequate permission to access the newly assigned Favorites menu. If all resources are not green, you can choose Allow All Permissions from the Actions menu. but remember that you are updating the resources for the role, not just this user.

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. 6.7
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.

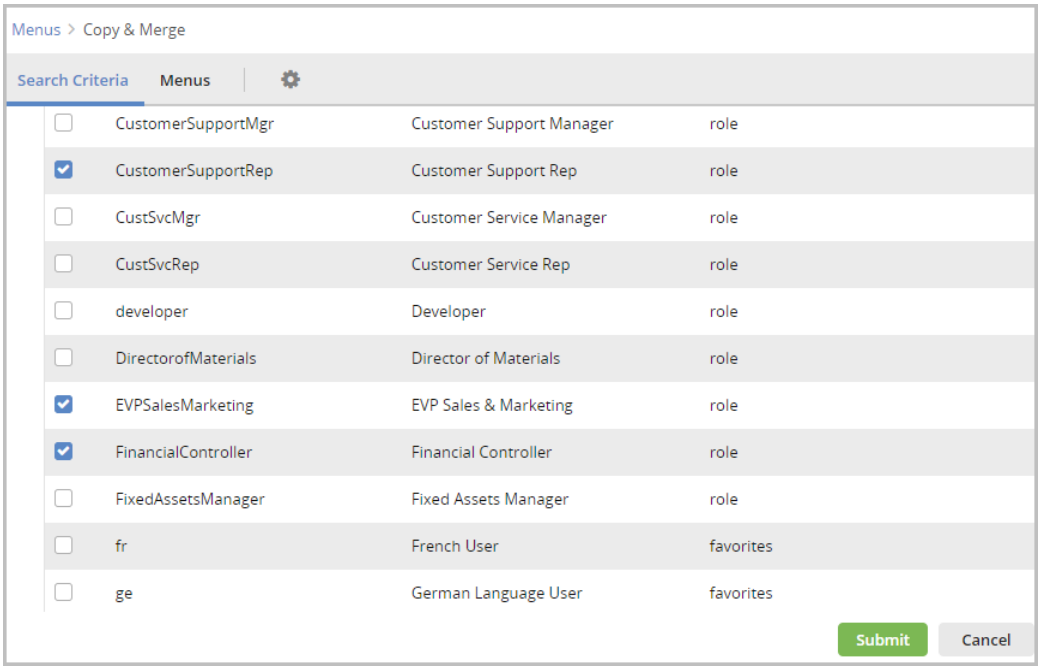
6 Click **Permissions** to check that the user's role has adequate permission to access the newly assigned Favorites menu. If all resources are not green, you can choose Allow All Permissions from the Actions menu, but remember that you are updating the resources for the role, not just this user.

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. 6.8
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 **Permissions**.

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 **Permissions** in the bottom right corner of a screen
- From other screens: by selecting the Permissions option from the More drop-down in the toolbar

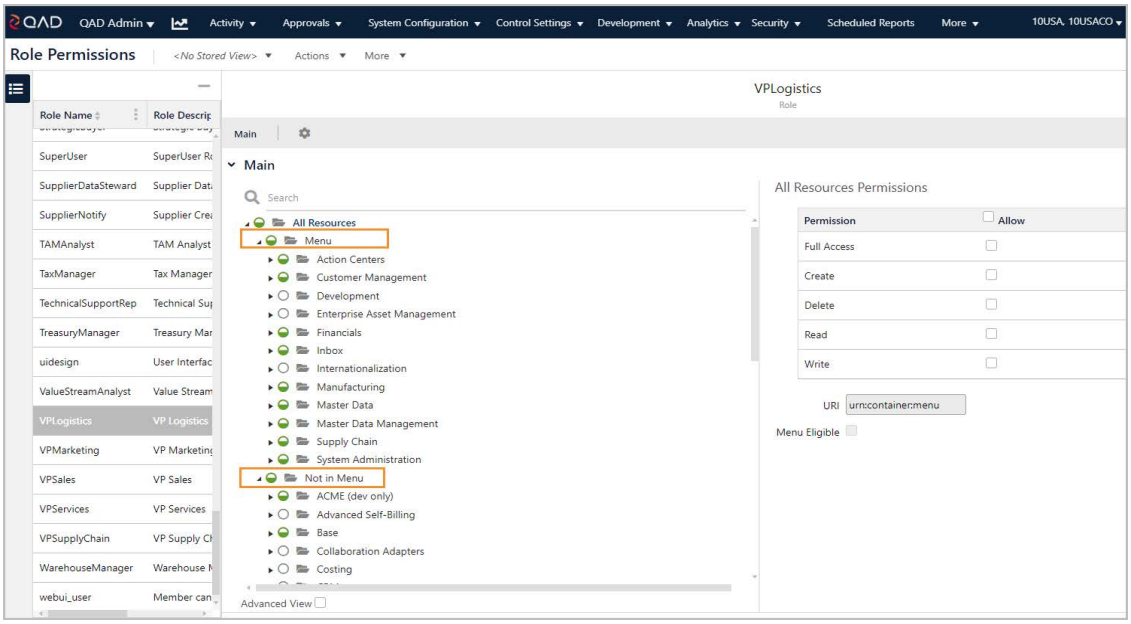
It is recommended to set up and configure permissions for QAD Adaptive using role menus and the Permissions option on individual screens. The Role Permissions tree is not intended to be used to set all permissions for a role and should be used sparingly.

QAD Adaptive 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 78 for more information. See "Fields and Field Groups" on page 98 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 6.9.

Fig. 6.9
Role Permissions



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

- Browse-only views

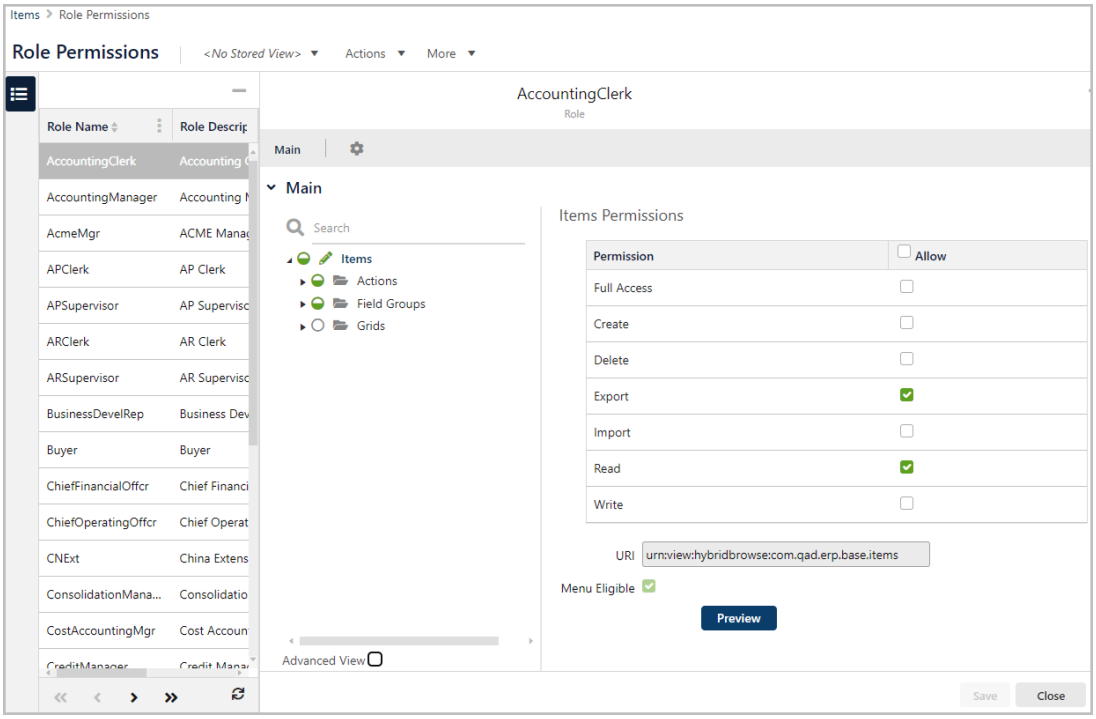
- Hybrid views
- Form-only views
- Reports
- URL links
- Action centers

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 6.10. 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. 6.10
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.

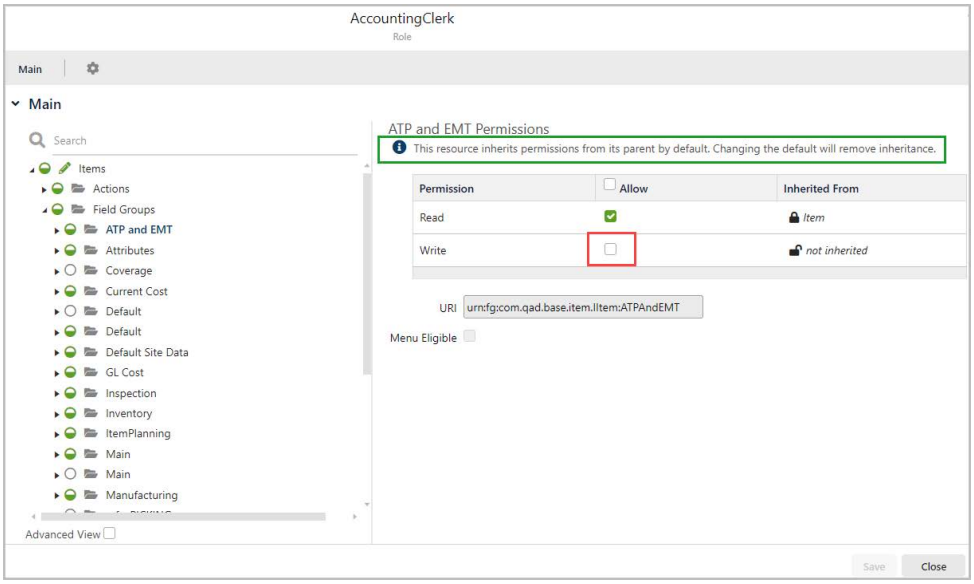
Field Permissions

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 6.11.

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

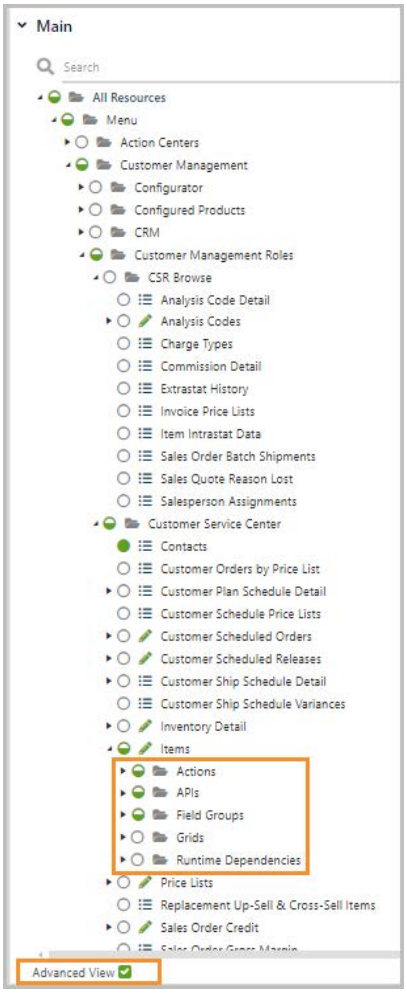
Fig. 6.11
Permission Inheritance for a Field Group



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 6.12 shows the expanded permission tree for the AccountingClerk role.

Fig. 6.12
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 96.

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. 6.13
Permissions Search

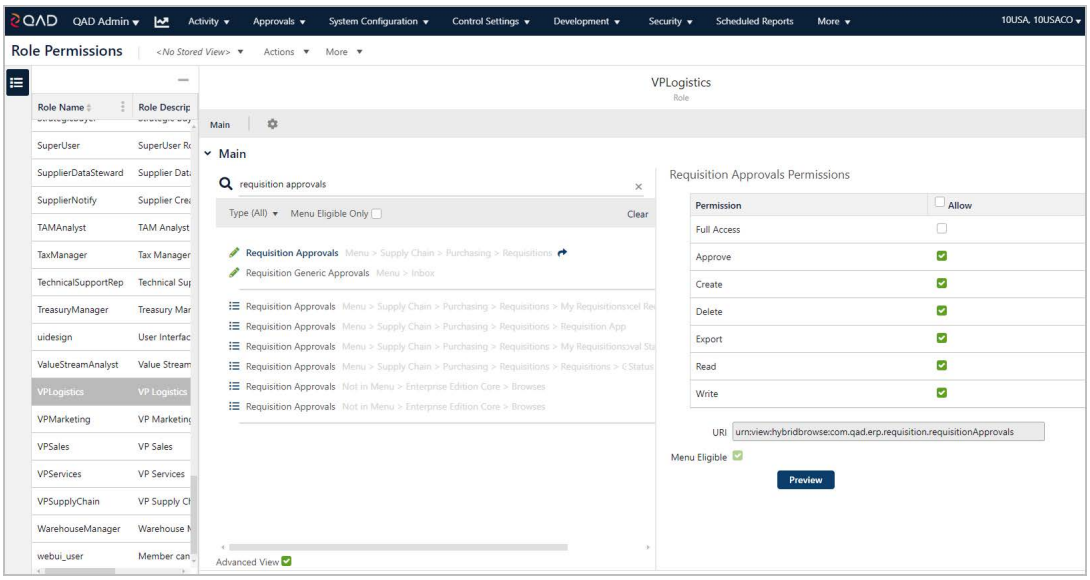
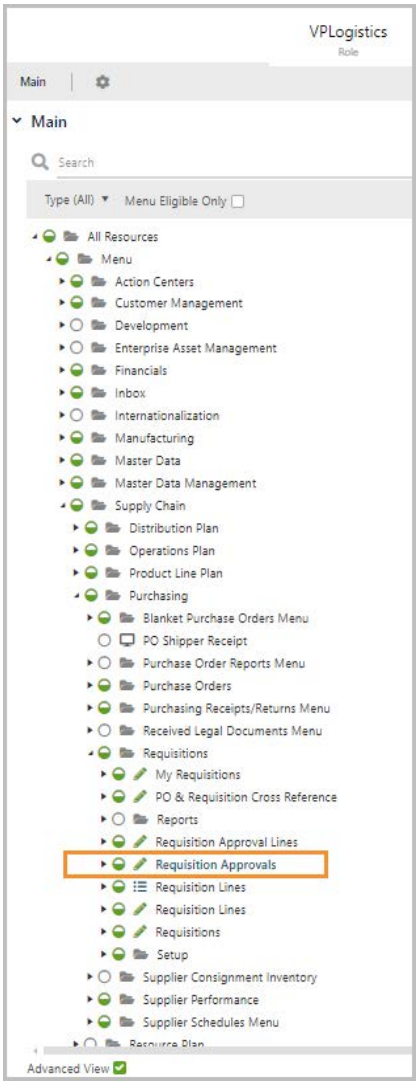


Figure 6.13 shows the search results for requisition approvals for the VP Logistics role. You can click the search result resources to view and update their permissions. If you need more information to determine which of the results is the one you are searching for, you can view each resource within the context of the permission hierarchy by selecting it and clicking the blue arrow next to it.

Fig. 6.14
Expanded View in Context

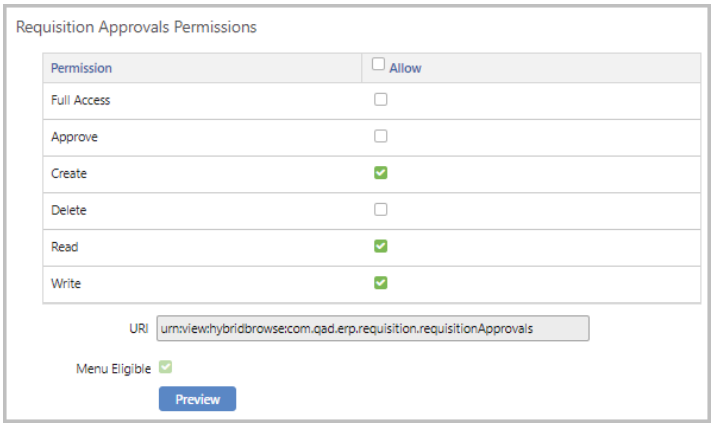


The permission tree expands to show where the resource, in blue, fits into the hierarchy, as shown in Figure 6.14.

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. 6.15
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 QAD Adaptive. 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 action is available from the Actions menu on the Role Permissions screen:

Refresh Permissions

The action clears all security-related caches and reloads permission data.

Assigning Permissions to Roles

QAD Adaptive securable resources are listed in the permission tree on Role Permissions. To access and view any of these components in QAD Adaptive, 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 78 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 QAD Adaptive 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 QAD Adaptive 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 a QAD Adaptive 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 100.

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

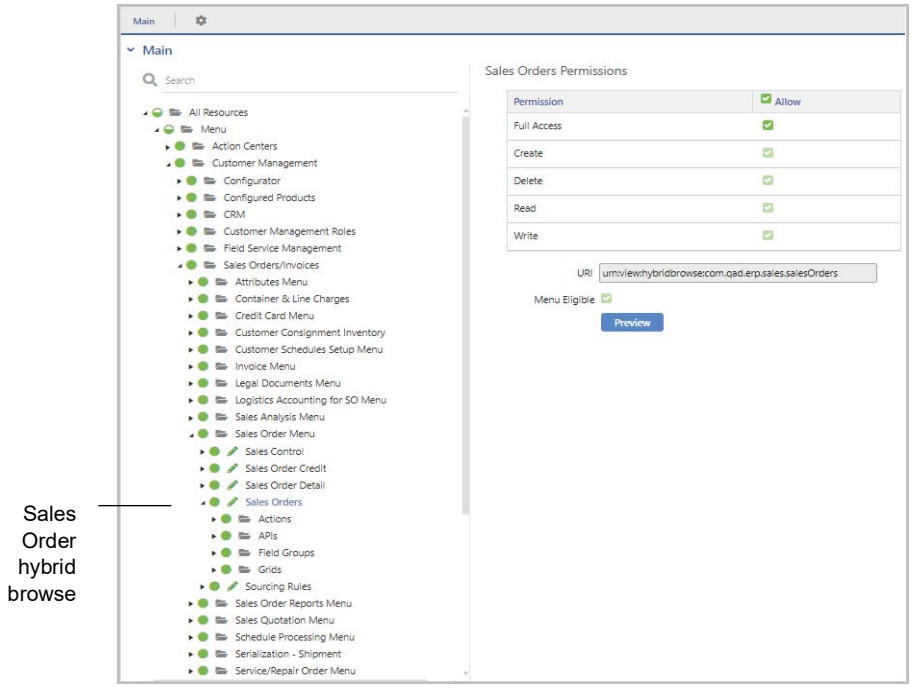
- "Hybrid Browse Screens" on page 94
- "Browse screens" on page 95
- "External Grids" on page 96
- "Lookups and Dashboard Panels" on page 97
- "Fields and Field Groups" on page 98

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 6.16. 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. 6.16
Hybrid Browse



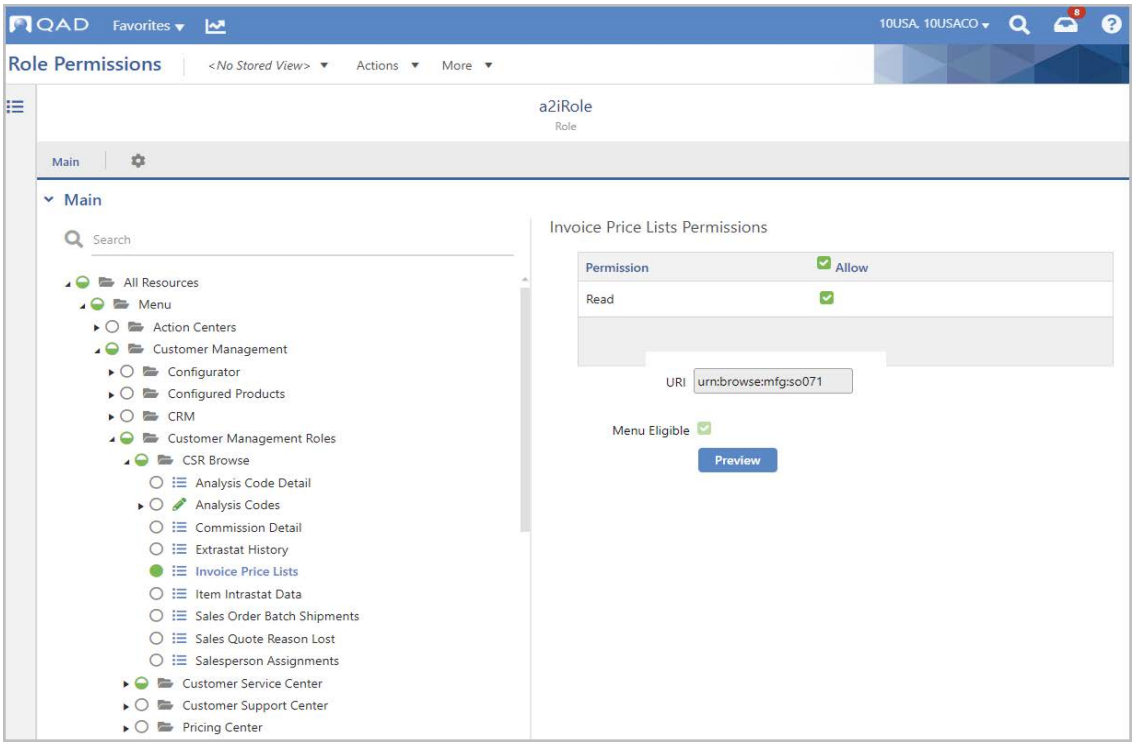
Browse screens

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 6.17.

Fig. 6.17
Invoice Price Lists Browse in the Permission Tree



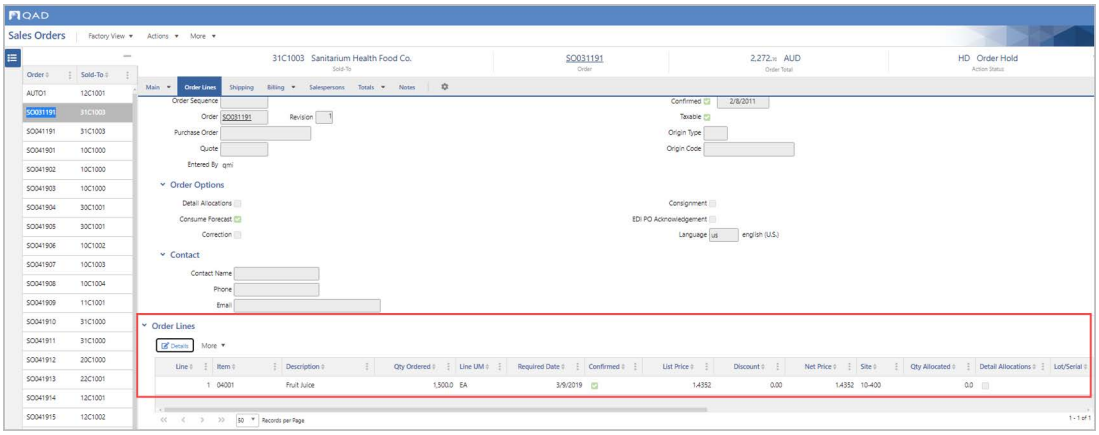
External Grids

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.

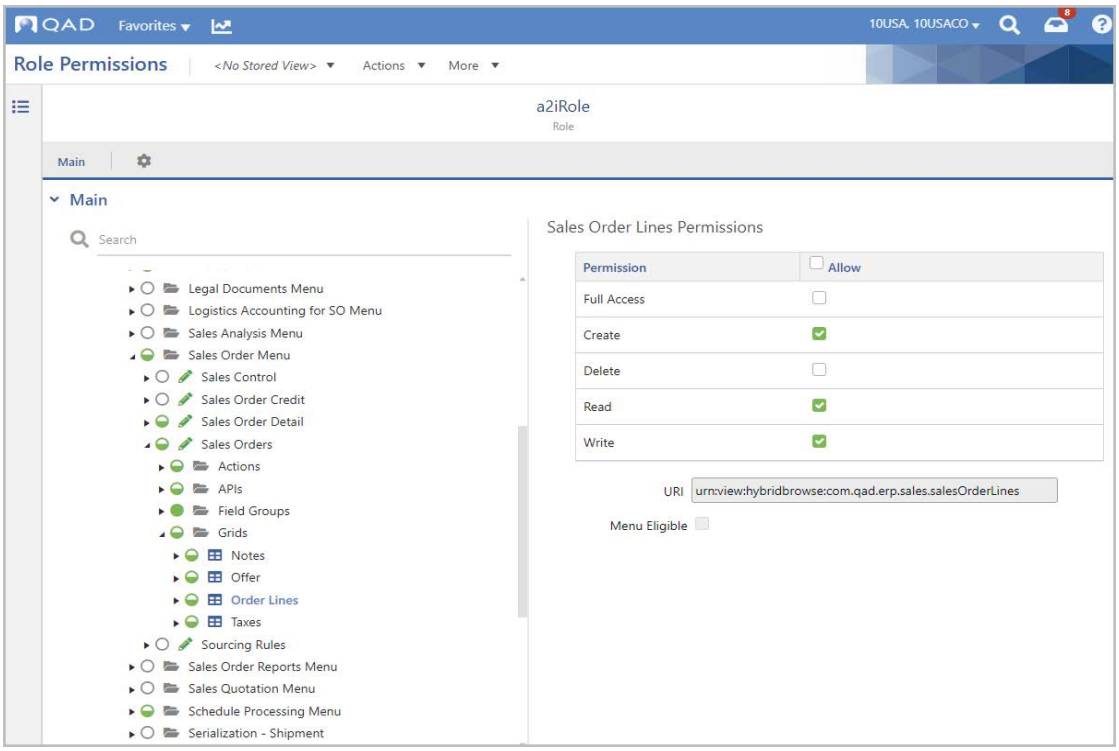
For example, the Order Lines external grid of the Sales Order hybrid browse shown in Figure 6.18 must be secured separately to provide complete access to the screen.

Fig. 6.18
External Grid



To secure an external grid, locate it in the permission tree, as shown in Figure 6.19, and assign corresponding permissions.

Fig. 6.19
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 QAD Adaptive. 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

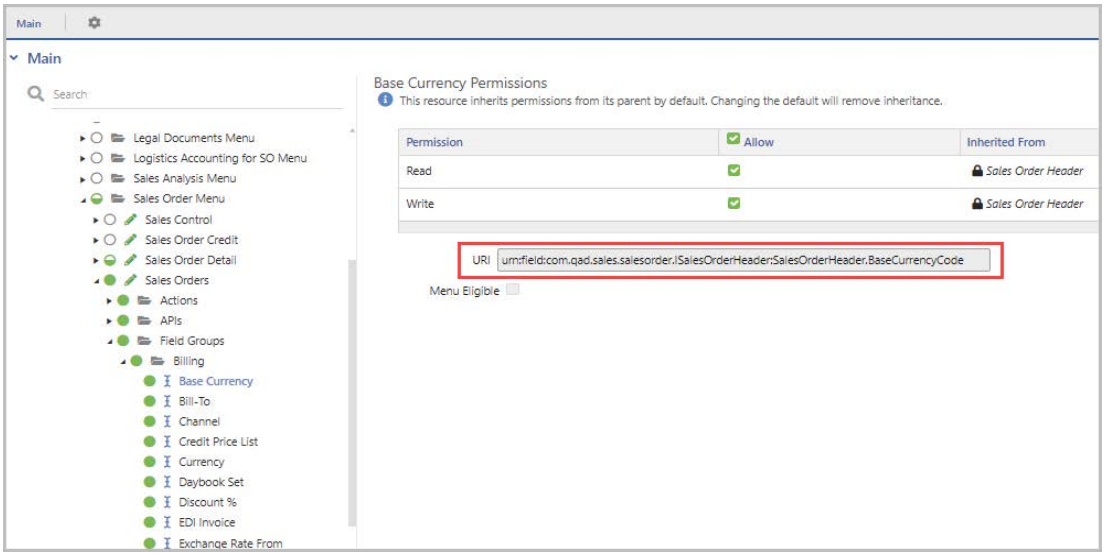
Individual fields and groups of fields are resources that can be secured. Fields and field groups only have read and write permissions. If you determine that more fields in your system need to be secured, contact QAD Services.

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

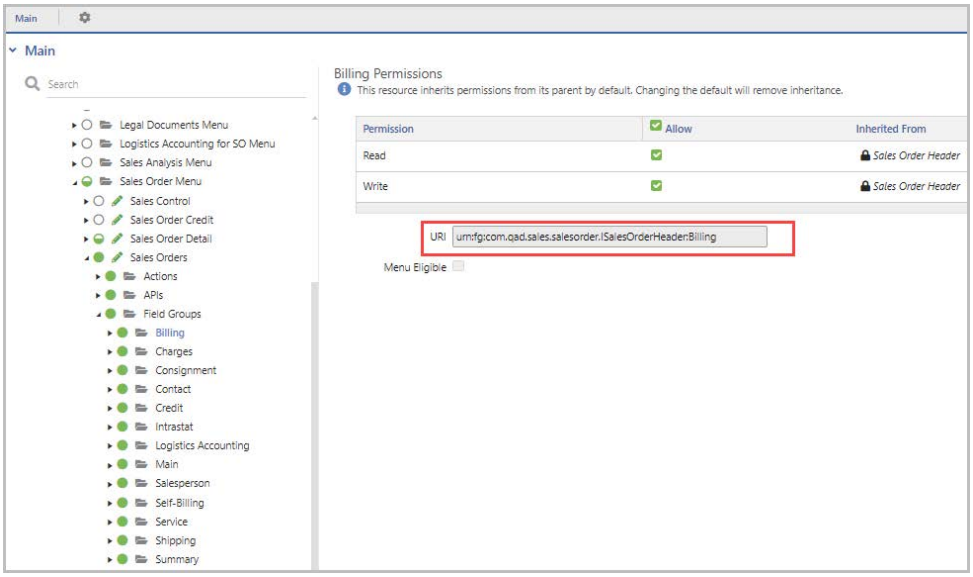
Fig. 6.20
Field Permission



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 6.21.

Fig. 6.21
Field Groups



Securing Fields and Field Groups from Within QAD Adaptive

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.

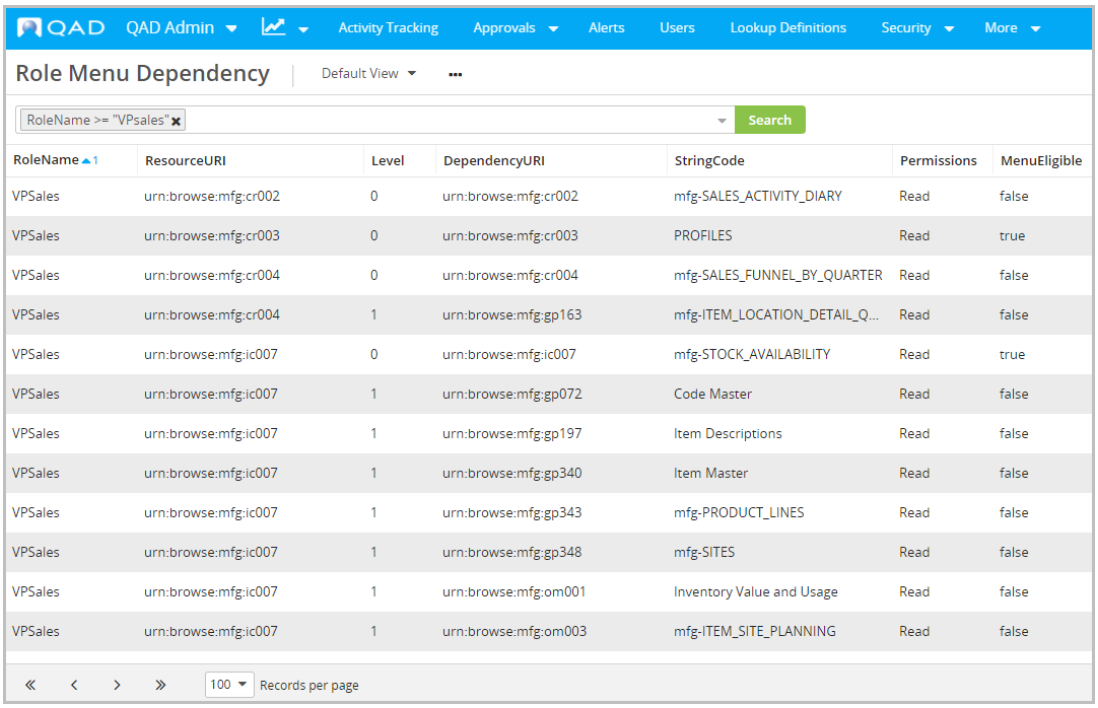
Manually Adding Resources

To add additional secured resources to QAD Adaptive, contact QAD Services or Support.

Role Menu Dependency

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

Fig. 6.22
Role Menu Dependency



RoleName. 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:

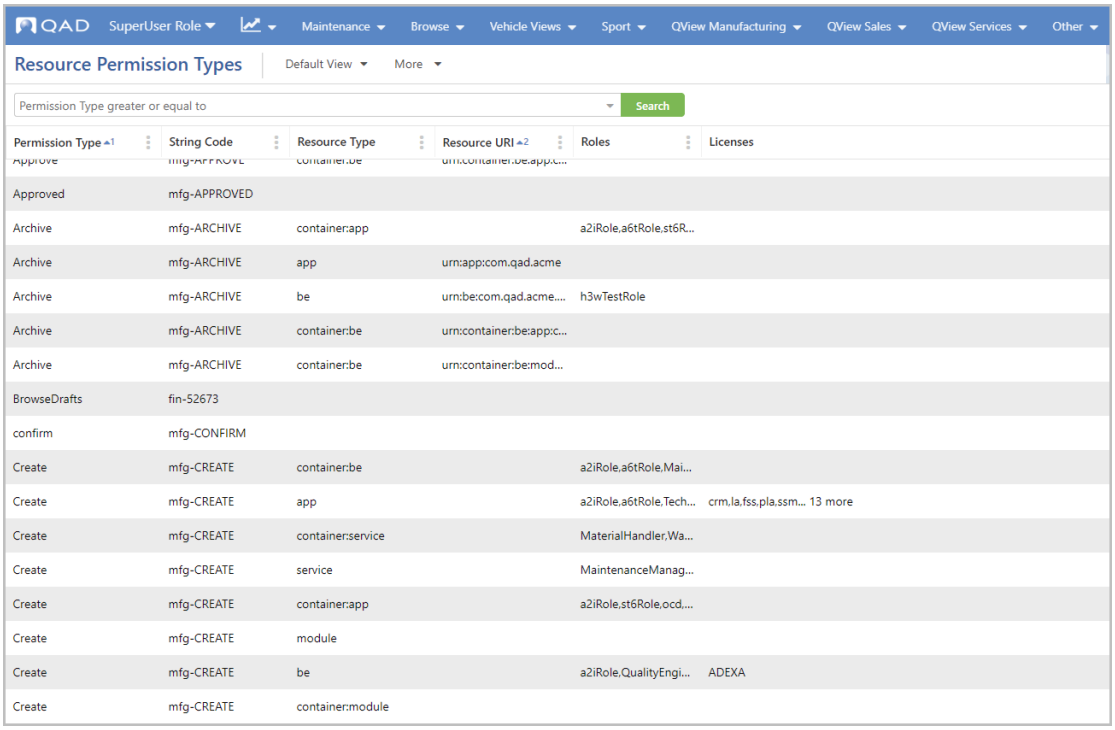
1. Navigate to the screen and select Permissions from the More menu.
2. In Role Permissions, edit the role requiring access.
3. Select Allow in the Permissions Grid for all of the listed resources.
4. Select Save.

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. 6.23
Resource Permission Types

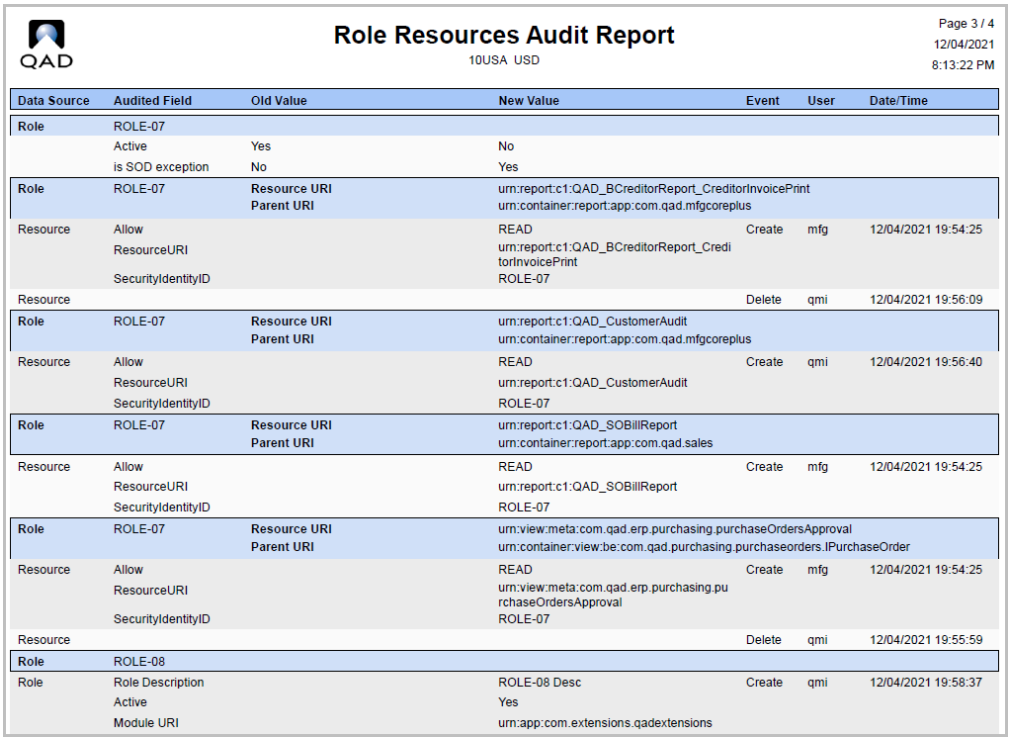


You can use the search functionality to determine which roles or licenses have access control entries for a specific permission type. For example, you can search the Full Access permission type and see all containers and resources that have Full Access assigned. The Resource Type column displays the 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 QAD Adaptive. The resources are listed as Resource and Enterprise Edition resources are listed as EE Resource in the report.

Fig. 6.24
Role Resource Audit Report



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** **Parent URI**	urn:report:c1:QAD_BCreditorReport_CreditorInvoicePrint 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** **Parent URI**	urn:report:c1:QAD_CustomerAudit 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** **Parent URI**	urn:report:c1:QAD_SOBillReport 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** **Parent URI**	urn:view:meta:com.qad.erp.purchasing.purchaseOrdersApproval 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. 6.25
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.purchaseOrders	
		Parent URI	urn:container:view:be:com.qad.purchasing.purchaseord	
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 6.25, 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 10, “Auditing,” on page 211.

Configure Stored Views Access

You can create and save customized screen layouts, called stored views, in QAD Adaptive. 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.

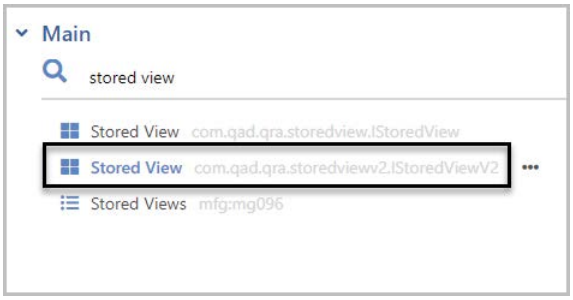
- System Level allows users to create and manage system-wide views that every user who has access to QAD Adaptive can view.
- Role Level allows users to create and manage role views that every user assigned to that role can view.
- User Level allows users to create personal views that only they can view 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 QAD Adaptive 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:

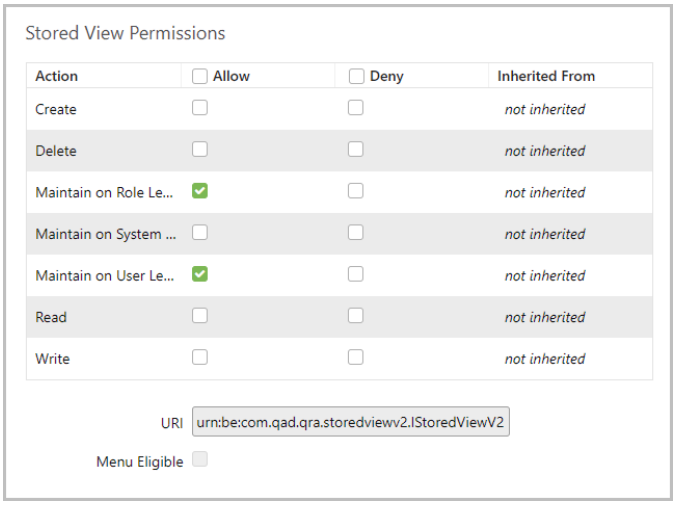
1. Double-click the role on Role Permissions.
2. In the Role Permissions Search menu, enter: **stored view**.
3. Select the result with the URI that ends with IStoredViewV2.

Fig. 6.26
Stored Views Search Result



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

Fig. 6.27
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 QAD Adaptive. Based upon a user's security permissions and the options selected in the Save Stored View As window on an QAD Adaptive screen, a stored view can be saved to a single domain or across multiple domains. See the Stored Views entry in the QAD Adaptive 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.

Note To allow a user to view all records, regardless of record-level security restrictions, assign them the Supervisor role.

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 QAD Adaptive 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 6.1
Search 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 QAD Adaptive, 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
```

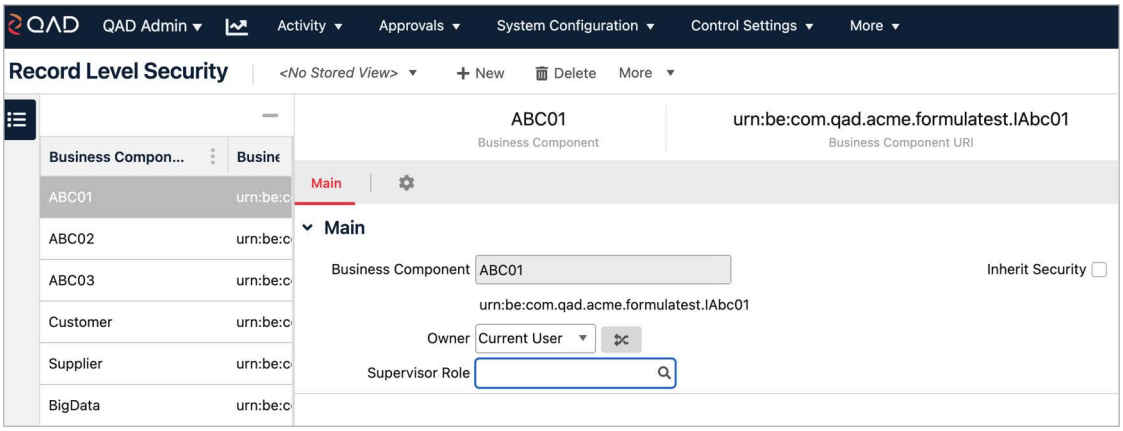
```
yab tomcat-webui-restart
```

Enabling Record-Level Security

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 Supervisor Role (defined in Record Level Security) or 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 110, before other users can view or edit secure records.

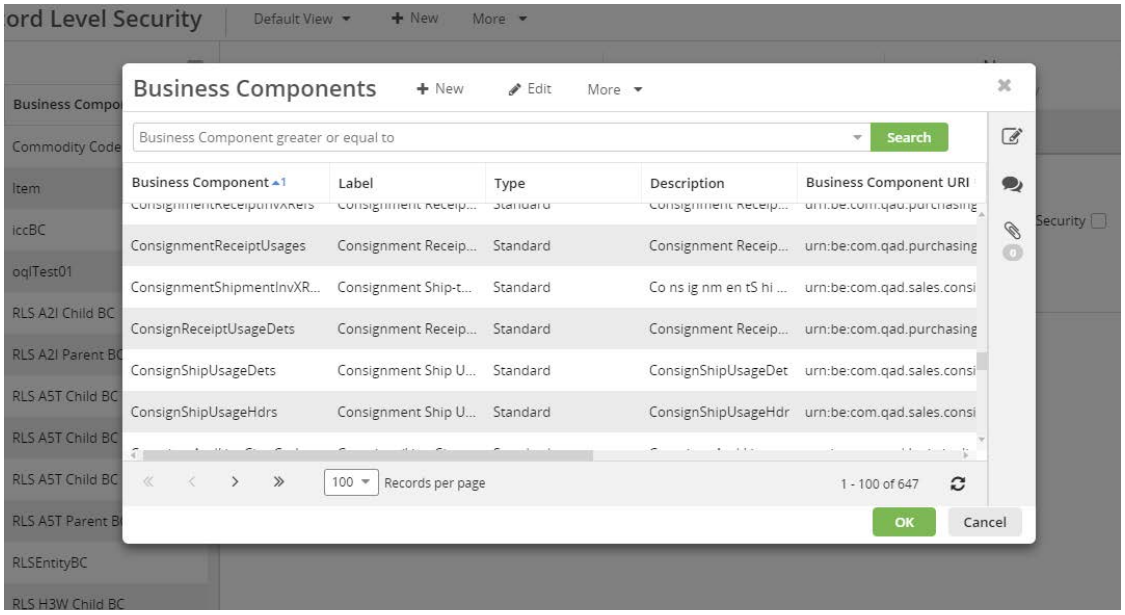
1 To enable record-level security for a business component, select New on the Record Level Security browse.

Fig. 6.28
Record Level Security



2 Select the business component from the lookup.

Fig. 6.29
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 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.

RLS Inheritance Improvement

Record Level Security (RLS) inheritance simplifies security rule configuration based on business component (BC) relationships.

If a business component is a child of a related BC with RLS enabled, you can configure it to inherit security from the parent. This means that security rules are only defined at the parent level—removing the need to configure rules for each child BC individually.

For example, Sales Order Header records can inherit security from the Salesperson business component. This way, a small set of Salesperson master records defines security for a much larger table of Sales Orders.

Depending on the structure of your data model, you may need to configure one-level inheritance or multi-level inheritance. When a child BC has no direct relationship with a parent, it can still inherit security through a chain of relationships.

Example: Sales Quote Lines -> Sales Quote Header -> Salesperson.

Migrating from regular RLS to inheritance RLS

To set up one-level inheritance for direct relationship between business components (for example, Sales Quote Header -> Salesperson), perform the following steps:

1 Clean up existing rules:

   a Remove all previously defined security rules for the related business components.

   b Delete any existing record-level security configurations for those components.

2 Create the relationship: in the Business Components screen, create the relationship from Sales Quote Header to Salesperson.

3 Configure RLS (in the correct order):

   a Create RLS for the root BC (Salesperson).

   b Create RLS for the Sales Quote Header and set it to inherit from the Salesperson.

4 Share records:

   a Open the Salesperson screen.

   b Select the record you want to share with a group or user.

   c Edit the record, click the **More** toolbar button and select **Share**.

5 Disable batch processing: set `qad-qracore.securityrules.processing.enabled=false`. This ensures that the Share action does not require batch processing.

In cases where the child BC has no direct relationship with the parent (for example, Sales Quote Line -> Salesperson), you can establish inheritance through intermediate components.

To set up multi-level inheritance (for example, Sales Quote Line -> Sales Quote Header -> Salesperson), perform the following steps:

1 Clean up existing rules:

   a Remove all previously defined security rules for the related business components.

   b Delete any existing record-level security configurations for those components.

2 Create the following relationships:

   a from Sales Quote Header to Salesperson.

   b from Sales Quote Line to Sales Quote Header.

   Note The relation should be N:1 (many to one) or 1-1 (one to one).

3 Configure RLS (in the correct order):

   a Create RLS for the root BC (Salesperson).

   b Create RLS for Sales Quote Header and set it to inherit from Salesperson.

   c Create RLS for Sales Quote Line and set it to inherit from Sales Quote Header.

4 Share records:

   a Open the Salesperson screen.

   b Select the record you want to share with a group or user.

   c Edit the record, click the **More** toolbar button, and select **Share**.

5 Disable batch processing: set `qad-qracore.securityrules.processing.enabled=false`. This ensures that the Share action does not require batch processing.

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

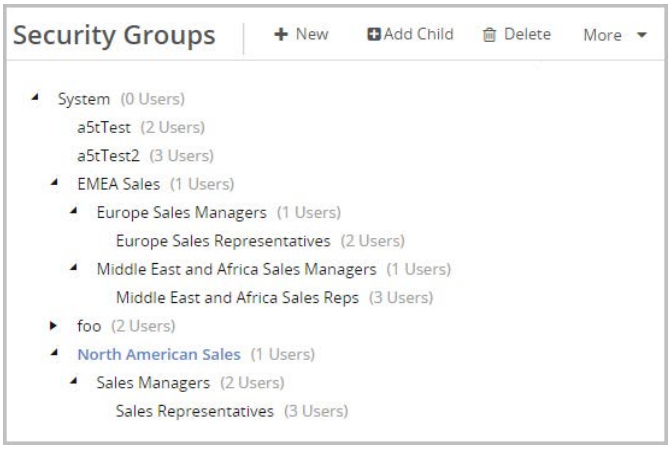
Security Groups

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 6.30, 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. 6.30
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.

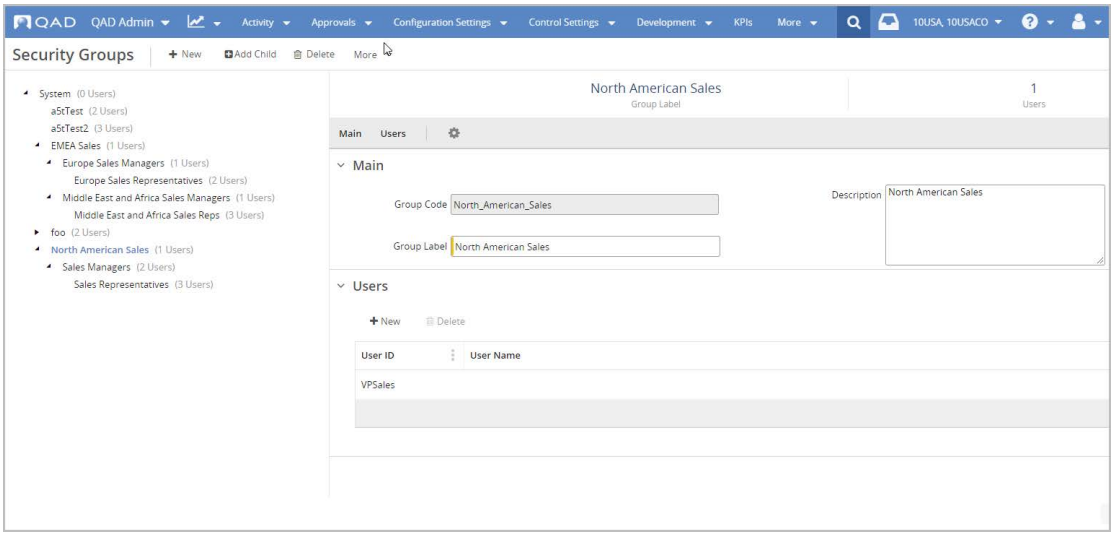
Delete

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. 6.31
Security Groups Main Panel



Main

The Main panel contains the following sections:

Group Code. The coded name for the group. This code must begin with a letter and contain 32 characters maximum. 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, click **New**. Then select a User ID from the lookup and click **Save**. To remove a user from the group, select the User ID in the Users grid and then click **Delete**.

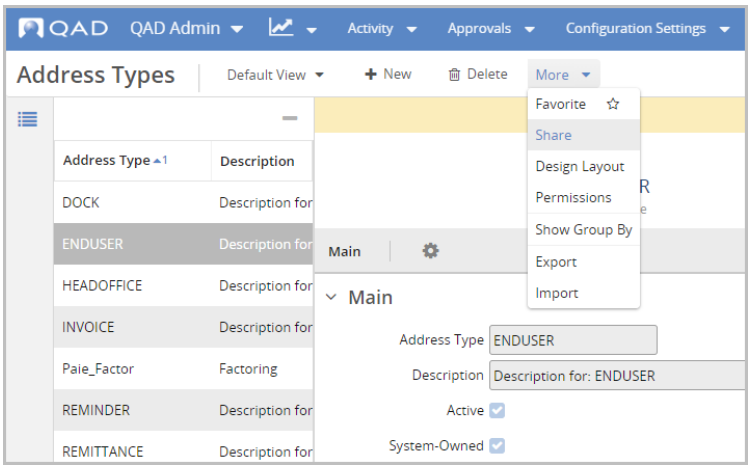
Note Level of access is always set at the role level, so even if a user is in a security group that has access to a record, if that user's role does not have access to the record's business component, the user cannot access the record.

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. 6.32
Share Access

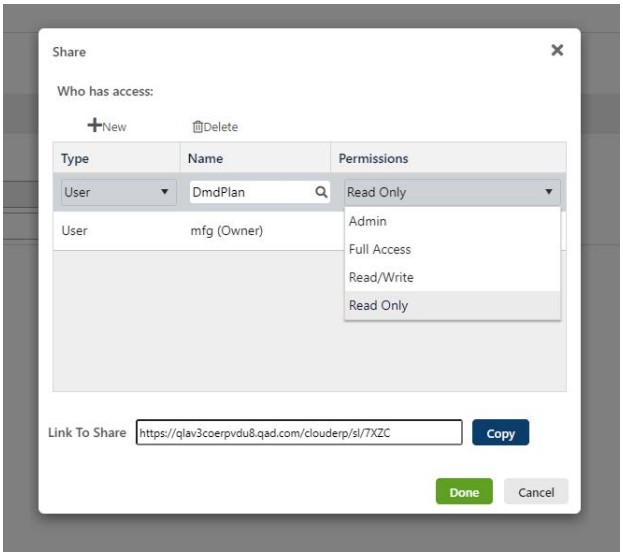


3. In the Share screen, first select the type of user who should have access to the record. You can choose Everyone, User, or Group if security groups are set up in the system.
4. Using the lookup in the Name column, select the individual user name or group name.

   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 the level of access the user should have. The following options are available:
   - 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. 6.33
Define Share Access



6 Click **Done** to grant access.

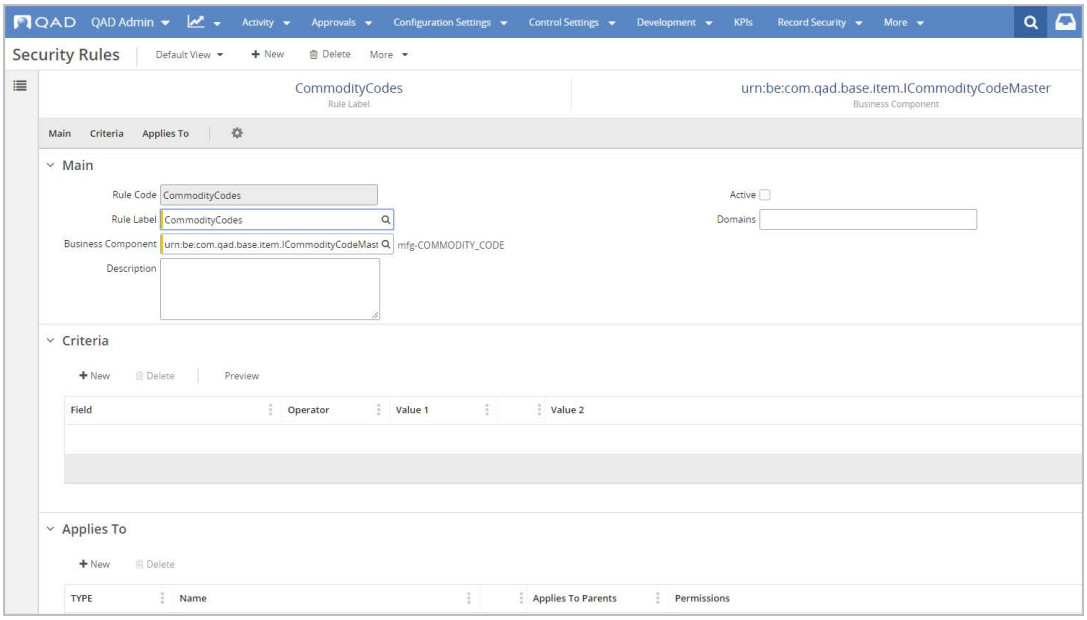
Note Users do not receive notification that they now have access to this record. This functionality is planned for a future release. Consider copying the Link to Share and sending the short link to the users who have received access.

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 are 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. 6.34
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.

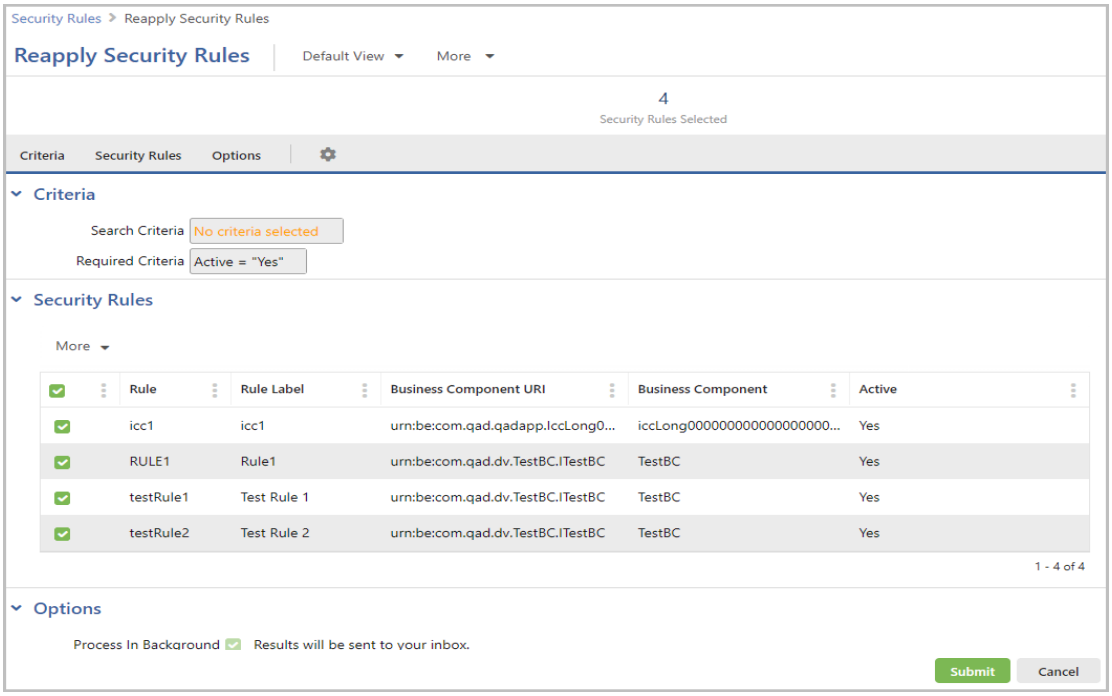
Reapply Security Rules

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. 6.35
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.

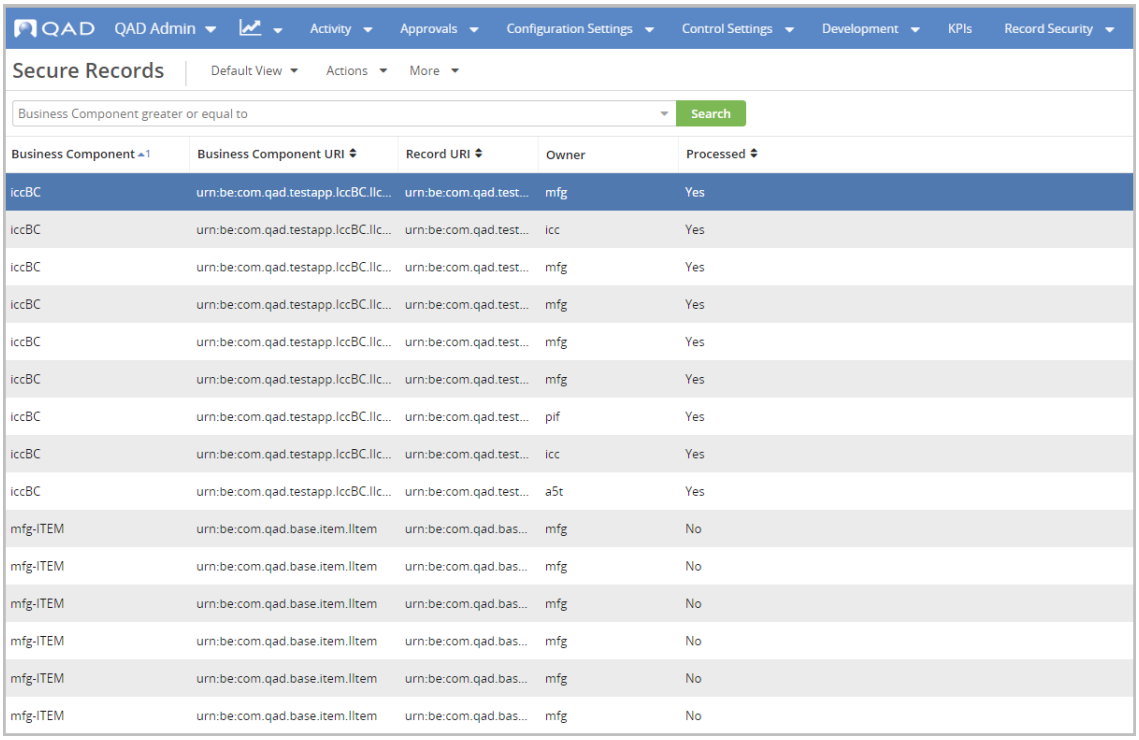
Options

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. 6.36
Secure Records



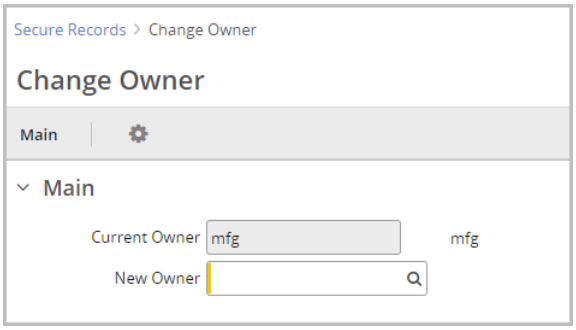
Use this browse to change the ownership of secure records, either as an individual or bulk action. This is useful if an employee leaves the company and you want to reassign all of that user's records to a new user.

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. 6.37
Individual Change Owner



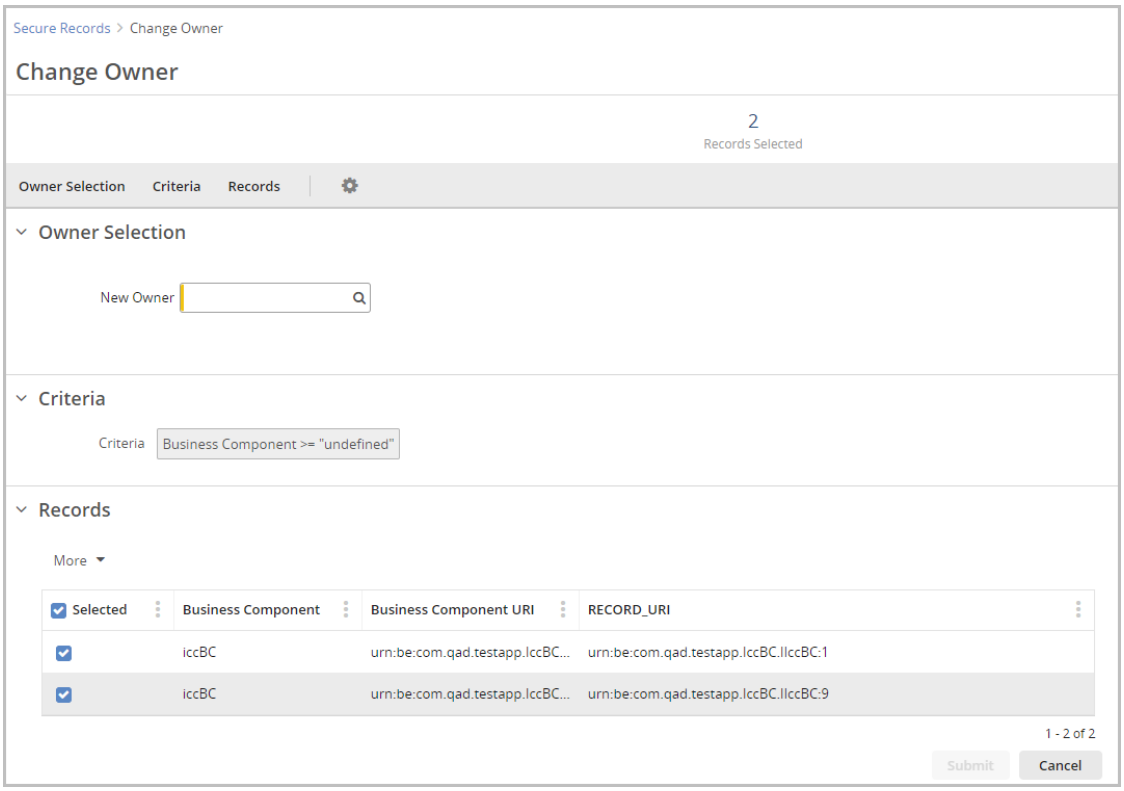
Choose the new owner from the New Owner lookup and then select Submit. The new owner now has full access to the record. It is important to remember that the previous owner no longer can access the record unless that user has been granted access through any method of sharing.

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. 6.38
Bulk Change Owner

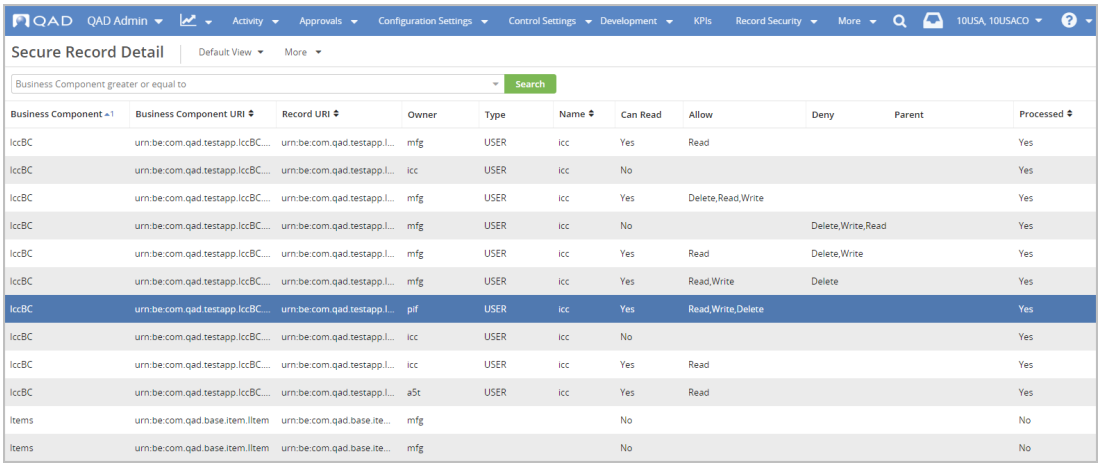


4. Select Submit to save.

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. 6.39
Secure Record Detail Browse



Important You can export and import Record Level Security configurations—including Security Groups and Security Rules—through the Configuration Data screen.

Chapter 7

Segregation of Duties in QAD Adaptive

This chapter describes how to configure and set up segregation of duties in QAD Adaptive. Segregation of duties is an internal control that prevents a single user from performing two or more phases of a transaction or operation.

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.

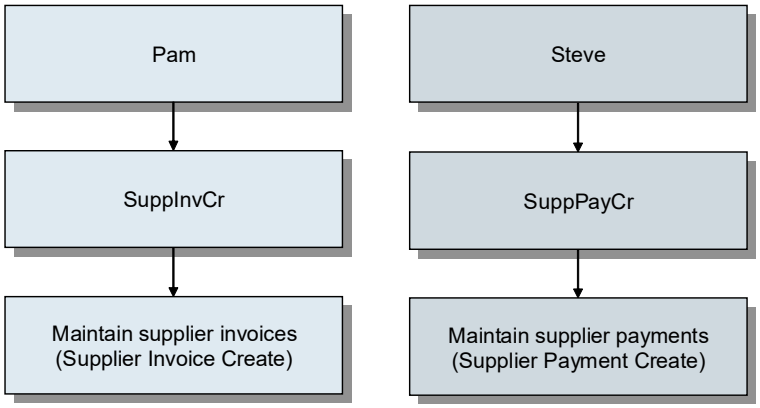
Segregation of duties refers to the notion that the duties of individuals in an organization should be limited to certain areas of responsibility, so as to minimize the ability of any individual to misappropriate company property. Segregation of duties prevents a single user from performing two or more phases of a transaction or operation. See “Segregation of Duties Verification” on page 124 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 7.1 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.

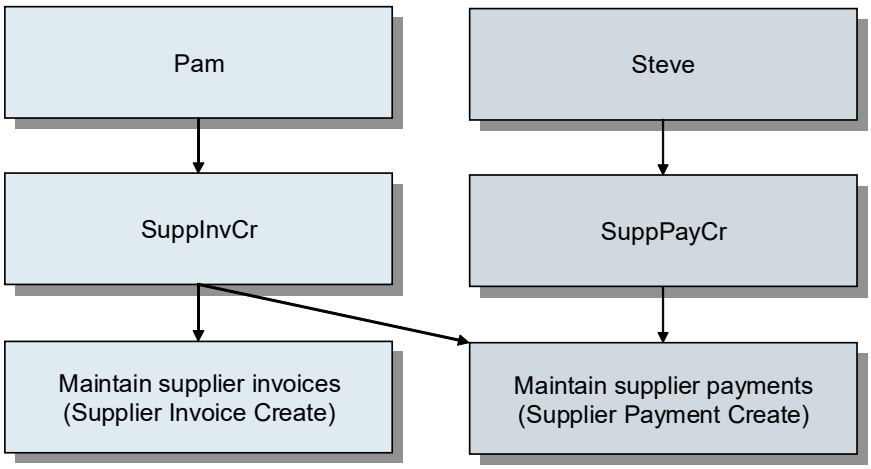
Fig. 7.1
Segregation of Duties Example



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 7.2 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. 7.2
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 128 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 145.

Segregation of Duties Policy Exceptions

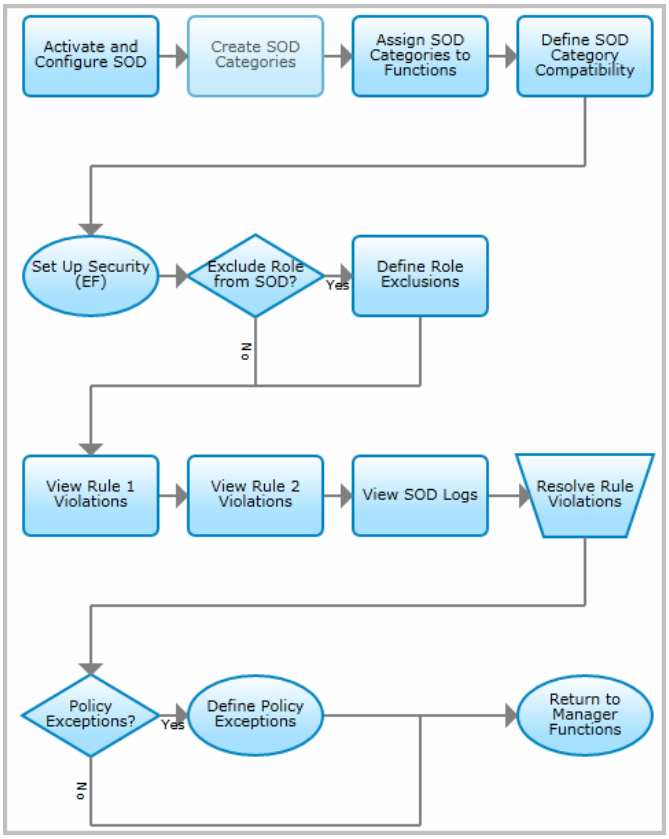
Segregation of duties permits policy exceptions to be defined to accommodate special circumstances—for example, when a business unit lacks sufficient personnel to adequately implement segregation of duties. Policy exceptions are defined on a user-by-user basis. That is, individual users can be given access to resources that are not compatible under your segregation of duties policy.

See “Maintain Segregation of Duties Policy Exceptions” on page 141.

Segregation of Duties Process Workflow

Use the options in the Segregation of Duties screens to set up segregation of duties and to configure segregation of duties functions. Figure 7.3 illustrates one possible segregation of duties process workflow; use it to set up segregation of duties functions in your environment.

Fig. 7.3
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 127. 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 135.

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 136.

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 139.

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 136.

The next step is to define role permissions in your system. This associates application resources to user roles. See “Role Menus” on page 78. 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 143.

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 141.

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 151.

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 154.

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 143.

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 143 for segregation of duties setup in QAD Adaptive.

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

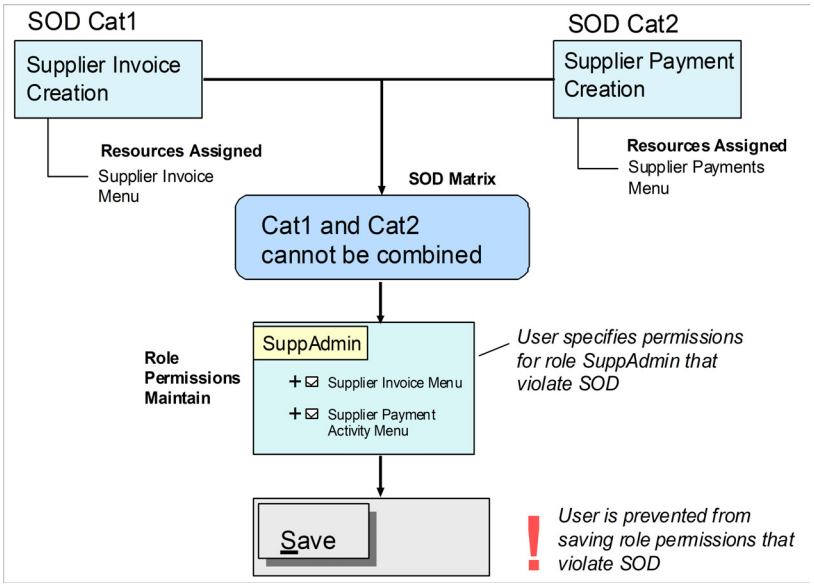
When you add a resource to the list of resources allowed for a role in Role Permissions, the system validates the assignment to verify that all the role resources belong to compatible segregation of duties categories (Rule 1 validation). If Rule 1 is violated, the system blocks the role permissions updates, 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. 7.4
Role Permissions Validation



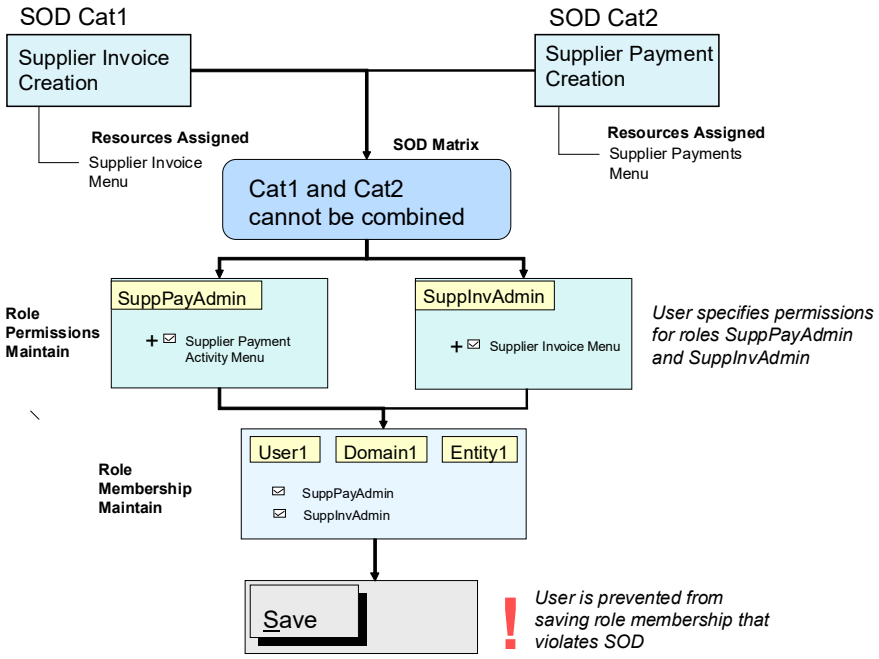
Role Membership Validation

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. 7.5
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.

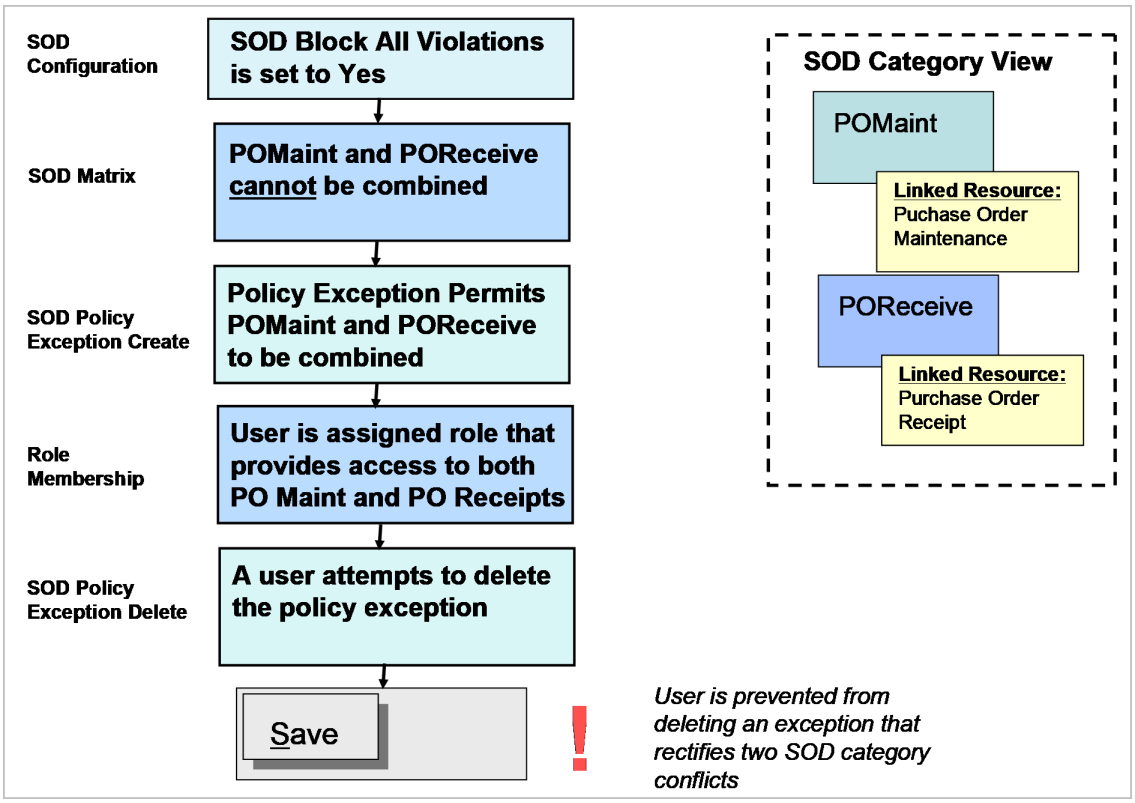
Indirect violations occur if you perform actions that violate segregation of duties rules using screens other than Role Permissions and User Access. However, role membership (Rule 2) violations caused by updates in Role Permissions are also examples of indirect violations.

Figure 7.6 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. 7.6
Indirect Segregation of Duties Violation



Segregation of Duties Rule Matrix

Table 7.1 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 7.1
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

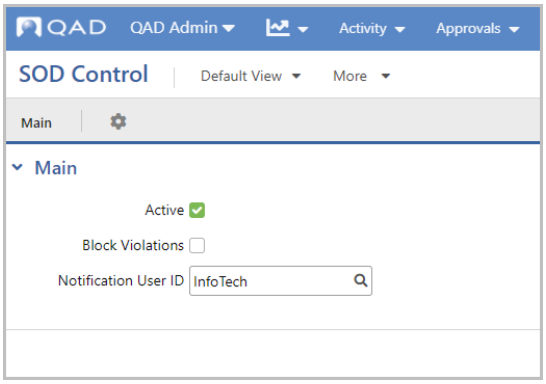
Before setting up segregation of duties, you must create user records in the system and provide basic identifying information. Access Users to define users in your system. Users must be defined in the system before they can be assigned to a role. See “Set Up Users” on page 58.

You can also define user roles—but not role permissions or role membership—as a prerequisite activity. See “Define Roles” on page 51.

Activate Segregation of Duties

Use SOD Control to activate segregation of duties rule checking on your system.

Fig. 7.7
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.

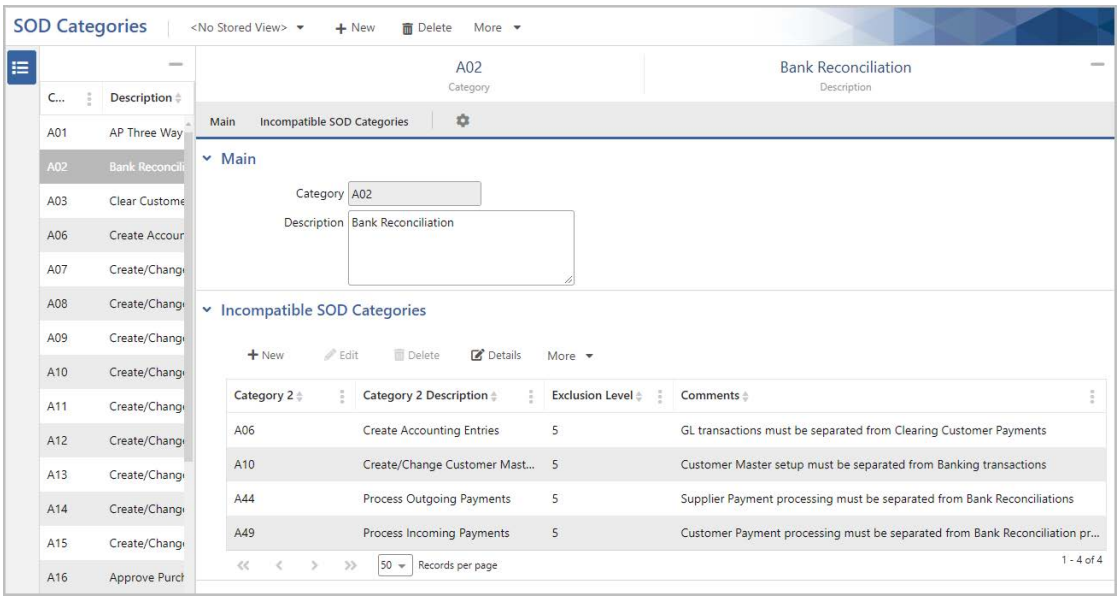
Notifications User ID. In addition to on-screen notifications and the SOD audit logs, the system can send notification of SOD violations to the User ID specified here. The notification can go to the user's external email address, the QAD inbox, or to both, depending on the Category Settings defined for 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. 7.8
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.

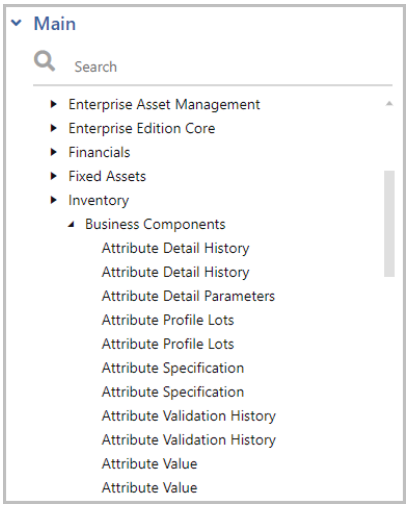
- If associated with no category, the resource is compatible with any other application resource, regardless of the SOD category to which those resources may be attached.

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. 7.9
QAD Adaptive 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.

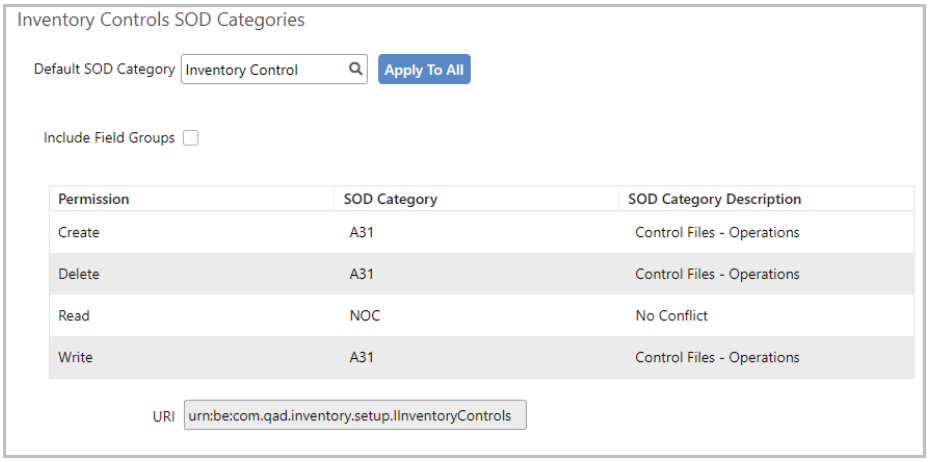
If you need more information to determine which result is the correct resource, you can view the resources within the context of the hierarchy.

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. 7.10
QAD Adaptive 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 58 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 144.

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.

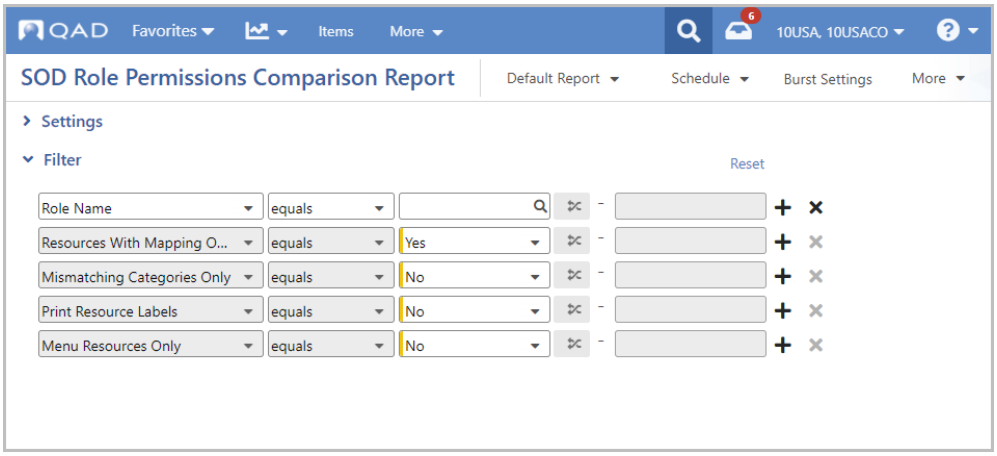
If you try to assign a user to a role that is incompatible with one or more of the roles already assigned to the user, when you attempt to update the database the system displays an error and does not assign the role.

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 QAD Adaptive by mapping Enterprise Edition resources to their equivalent QAD Adaptive resources.

Fig. 7.11
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 **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 QAD Adaptive Resource URI and its corresponding SOD category, and the assigned permission type.

Mismatching Categories Only. This filter removes the EE and QAD Adaptive resources that are identical and shows only those resources that have different SOD categories in Enterprise Edition and QAD Adaptive.

Print Resource Labels. This filter replaces the resource URI with menu titles for Enterprise Edition and resource labels for QAD Adaptive.

Menu Resource Only. This filter returns the mapping of Enterprise Edition resources to menu-eligible resources in QAD Adaptive. 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 70.

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.

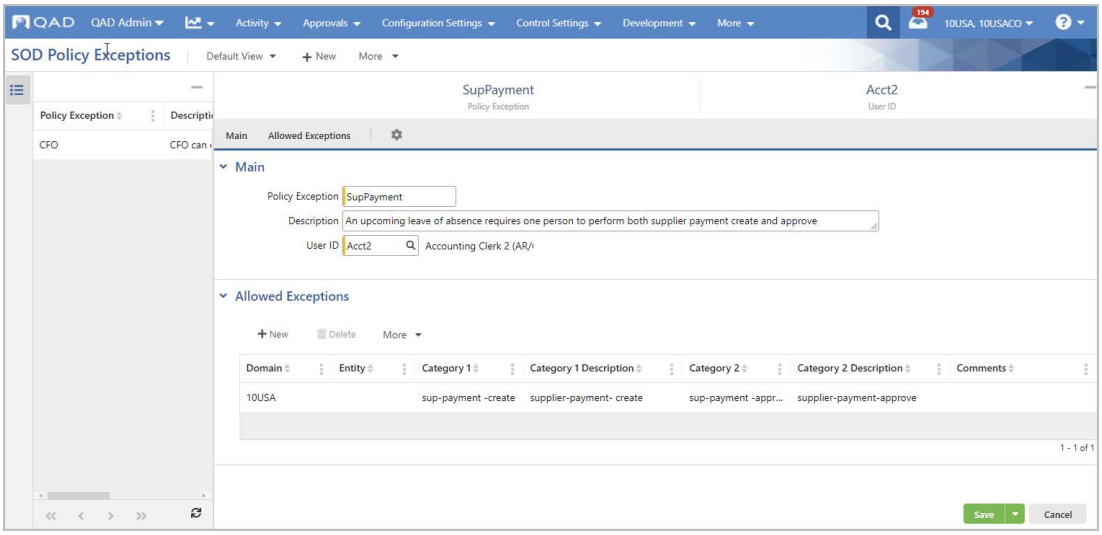
Policies are checked any time a change is made that impacts segregation of duties; for example, when a user is assigned to a role, when you link resources to categories, when you change role permissions, or when you change role membership.

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. 7.12
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.

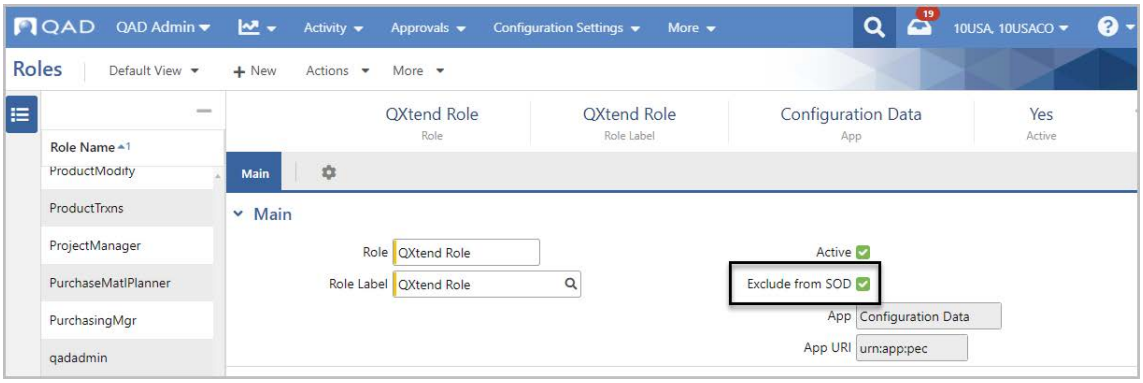
Segregation of Duties Role Exclusions

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 7.13, 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 QAD Adaptive Role” on page 52 for details on creating new roles.

Fig. 7.13
Exclude from SOD



SOD Setup

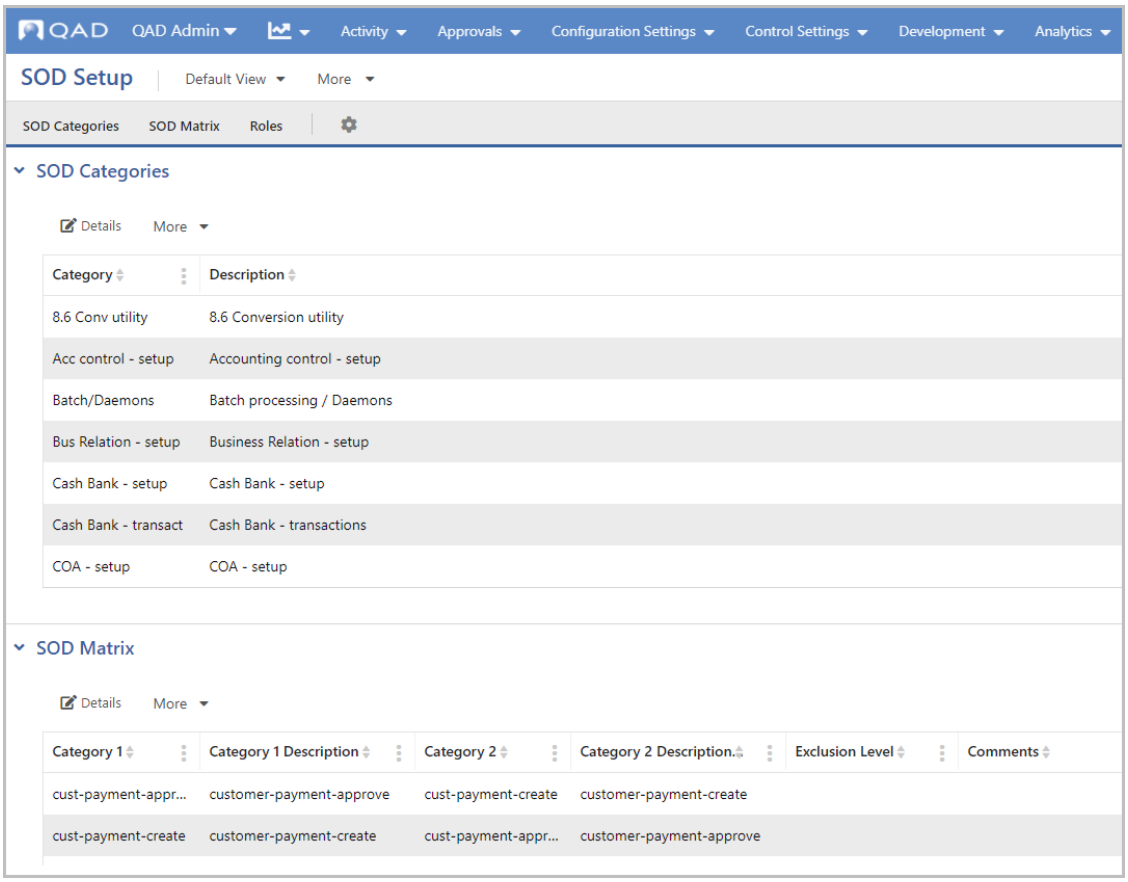
SOD Setup brings together SOD categories, the SOD matrix of incompatible categories, and system roles. From this screen, you can load default data for segregation of duties categories, matrices, menus, resource assignments, and roles using a single Excel spreadsheet. The import function lets you check 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 146 for more information on Excel integration.

Fig. 7.14
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 QAD Adaptive 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 QAD Adaptive. 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.

QAD Adaptive resources can have multiple permissions assigned to them, such as Read, Create, and Delete. Because of this permission granularity, one QAD Adaptive 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

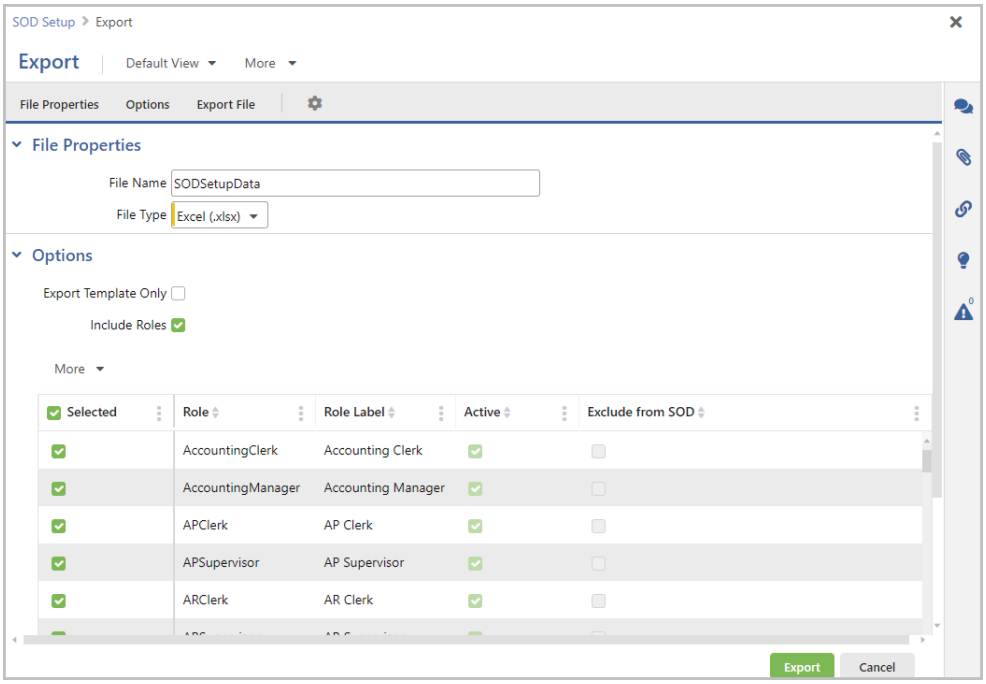
The Role sheet lists the roles that were selected during export, if any. You can edit existing roles and add new roles to be included in the system when the file is imported. For each role, you can indicate if the role is active or inactive, and indicate if any roles are excluded from segregation of 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. 7.15
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 7.15, 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.

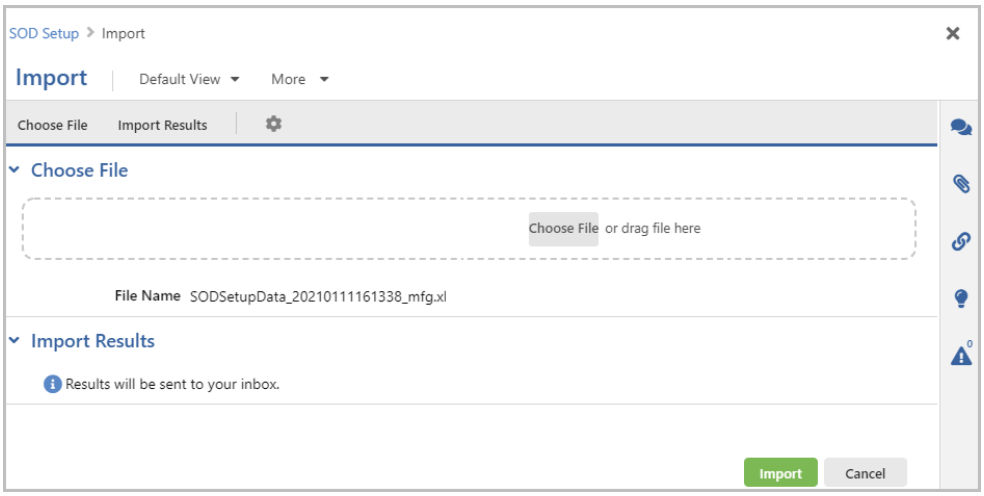
Import to SOD Setup

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. 7.16
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

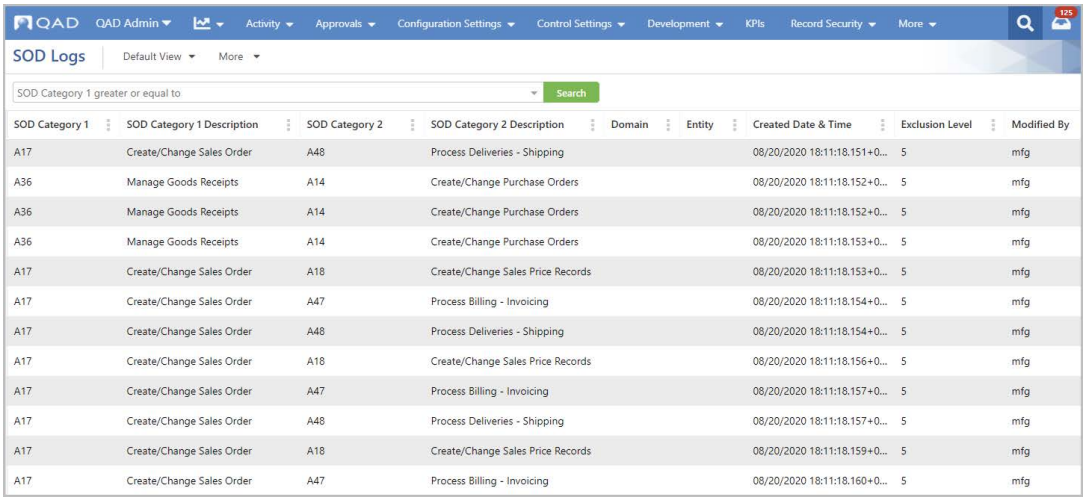
View Log History

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. 7.17
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.

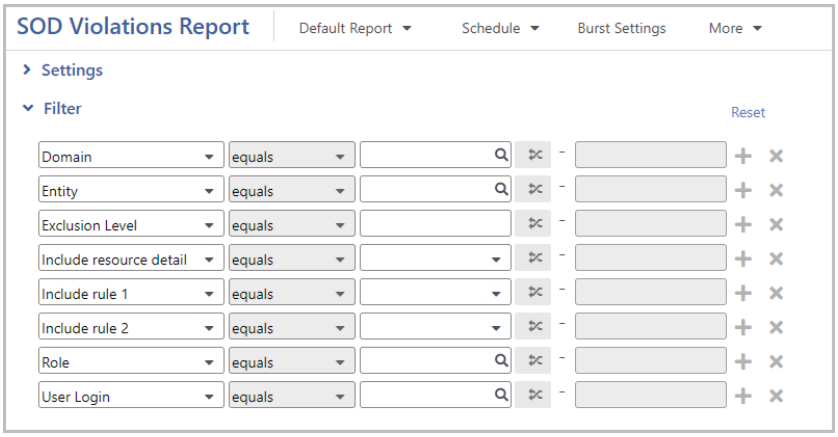
The report has the following filter fields:

- Entity
- Domain
- Role
- User

- Include rule 1 (Yes/No)
- Include rule 2 (Yes/No)
- Exclusion Level
- Include Resource Details (Yes/No)

Figure 7.18 illustrates the selection criteria for the SOD Violations report.

Fig. 7.18
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

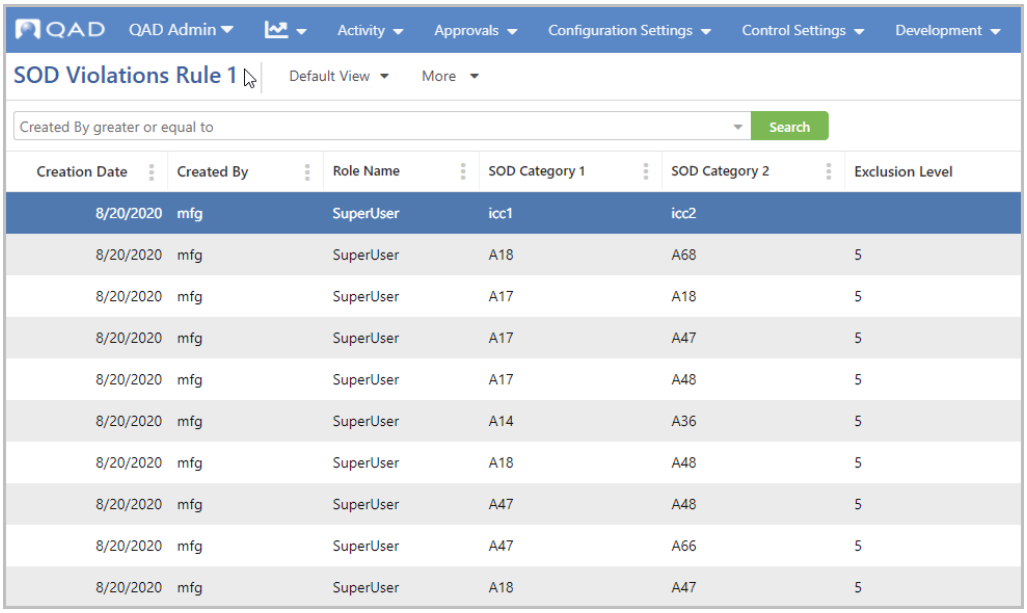
Category codes are displayed with their description. Resources are displayed with their corresponding menu entry and label.

Fig. 7.19
SOD Violations Report

View Role Permissions Violations

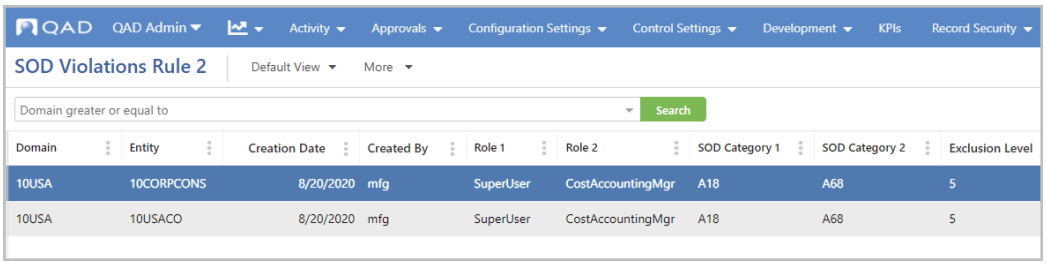
Use SOD Violations Rule 1 to display details of role permission violations.

Fig. 7.20
SOD Violations Rule 1



Use SOD Violations Rule 2 to display details of role membership violations.

Fig. 7.21
SOD Violations Rule 2



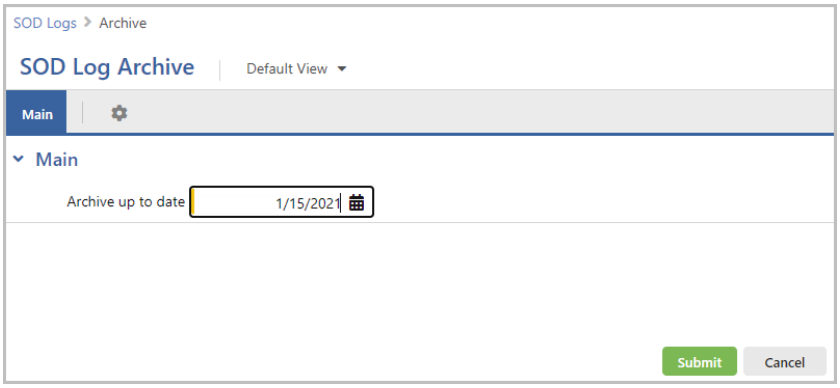
Archive Log Record Files

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. 7.22
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 8

Electronic Signatures in QAD Adaptive

This section discusses how to set up and use electronic signatures functionality in QAD Adaptive.

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 QAD Adaptive 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 78.

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 QAD Adaptive, 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 QAD Adaptive, 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 QAD Adaptive 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 158.
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 158.
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 159.
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 164.

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

Note You can export and import the eSignature configurations using the Configuration Data screen. This functionality allows the configurations to be propagated between environments.

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 166.

Use Reason Codes to define signature reason codes that are appropriate to your environment.

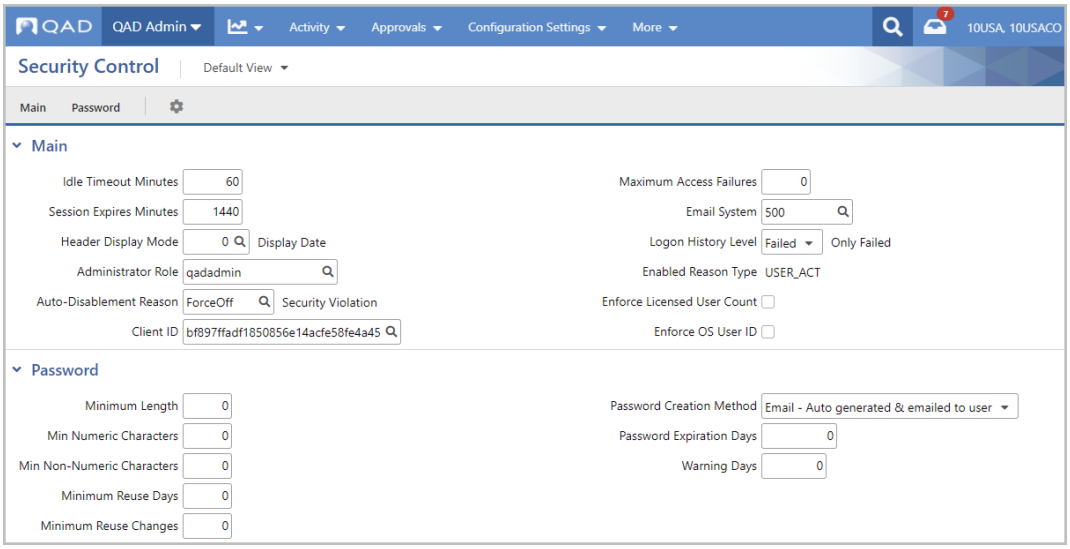
Important All reason codes used by electronic signatures must be associated with the QAD-provided ESIG reason type. Reasons of any other type cannot be entered in the signature prompt frame.

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 15 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. 8.1
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. You can specify any value from 1 to 20. The default field value is 10. For more information, see "Define General Security Settings" on page 30.
- 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 QAD Adaptive" on page 99 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 8.1
Default Electronic Signature Configurations

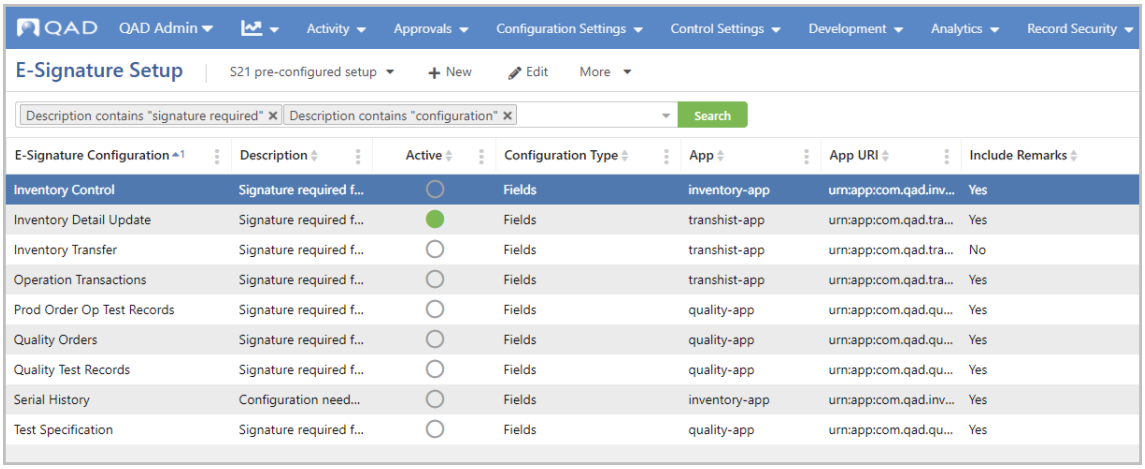
Configuration Name	Change Requiring a Signature
Asset Work Order Close	An asset work order is closed
Inventory Control	Changes are made in the Compliance panel to any of the following: • Compliance Active • Modify Component Issue • Modify Co/By Product Receipts • Lot Control Level • Single Lot per Purchase 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

Configuration Name	Change Requiring a Signature
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
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.

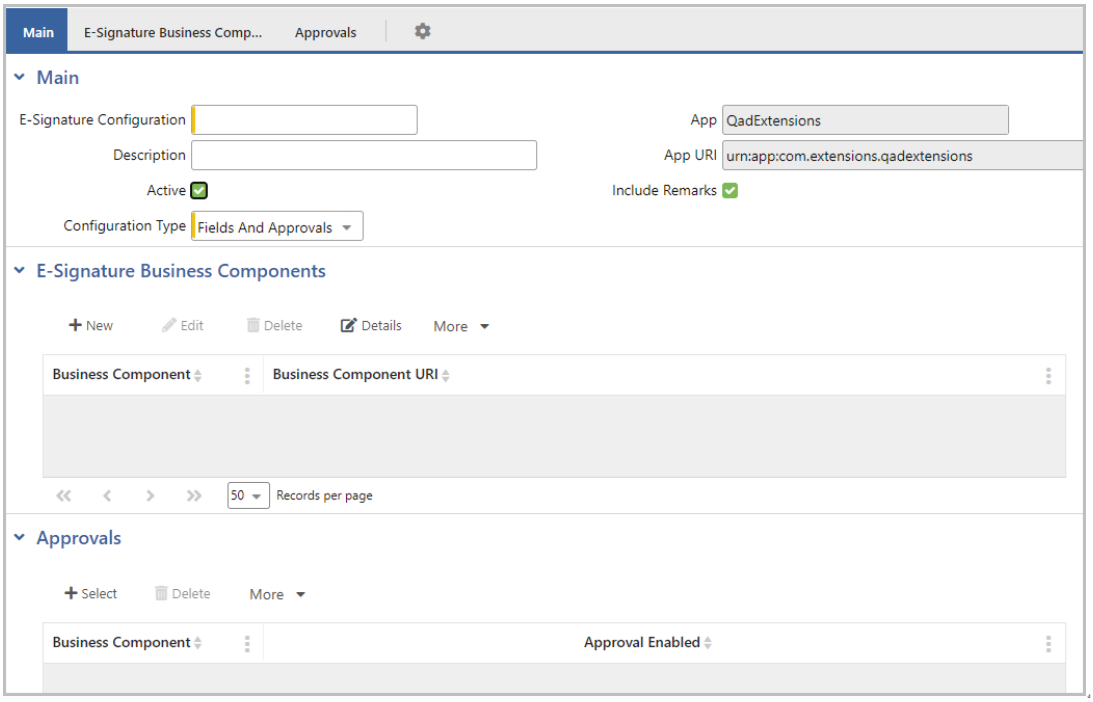
Fig. 8.2
E-Signature Setup



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. 8.3
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

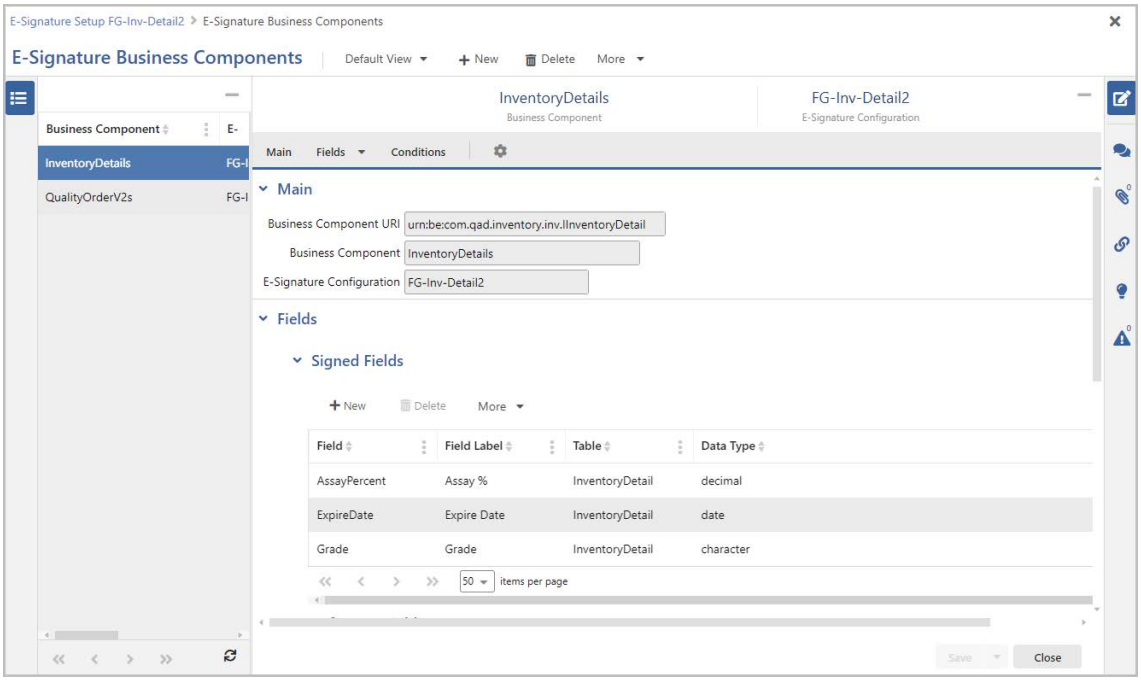
The Approvals option is visible if you selected Approvals or Fields and Approvals in the Configuration Type drop-down menu in E-Signature Setup.

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. 8.4
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.

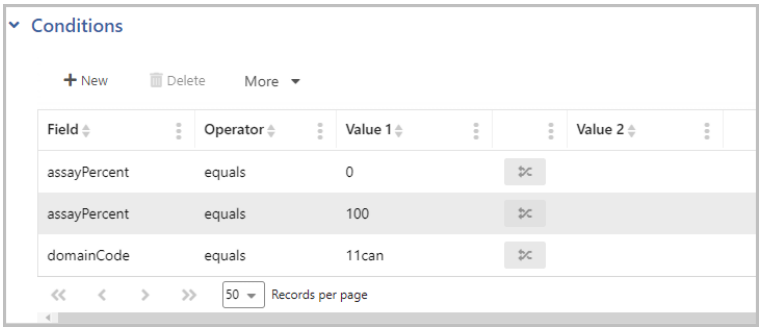
Data Type. The data type of the selected field, such as decimal, date, or character.

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 166.

Conditions

Use the Conditions grid to limit the scope of the electronic signature configuration.

Fig. 8.5
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.

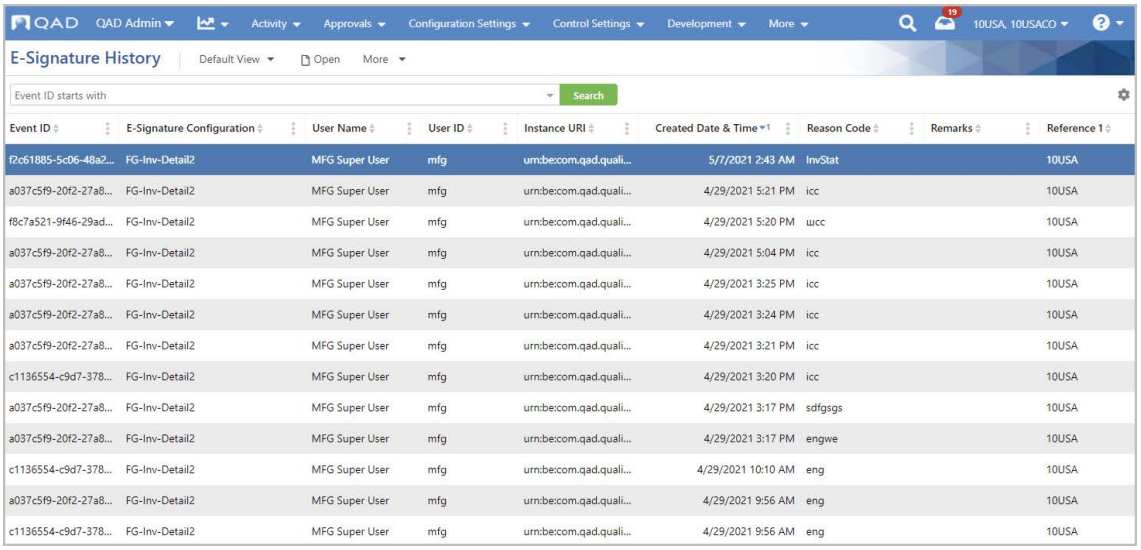
Value 2. If required, enter a second value.

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 166.

E-Signature History

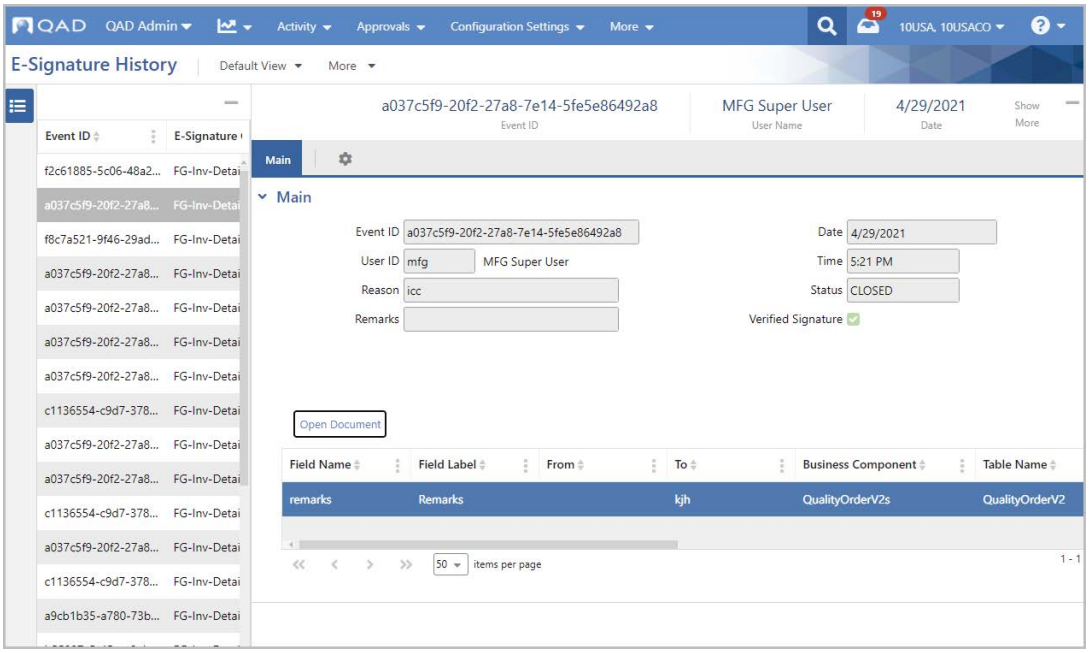
You can use E-Signature History to review changes made to electronic signature-enabled fields. Each historical record includes the field’s original content and its changed content, along with the user ID of the user who made the change, the time and date of the change, and the reason for the change.

Fig. 8.6
E-Signature History



To view the details of an event ID, double-click the record.

Fig. 8.7
E-Signature History Details

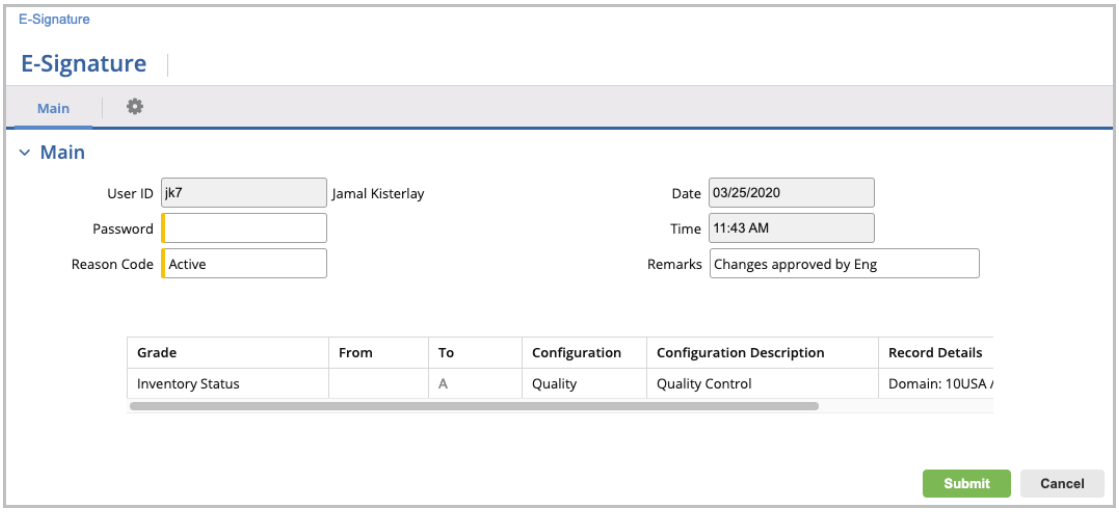


The individual record displays the data tied to this electronic signature event and links to the document that was changed. Click the **Open Document** link, highlighted in Figure 8.7, to open the record where the change was made.

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. 8.8
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.

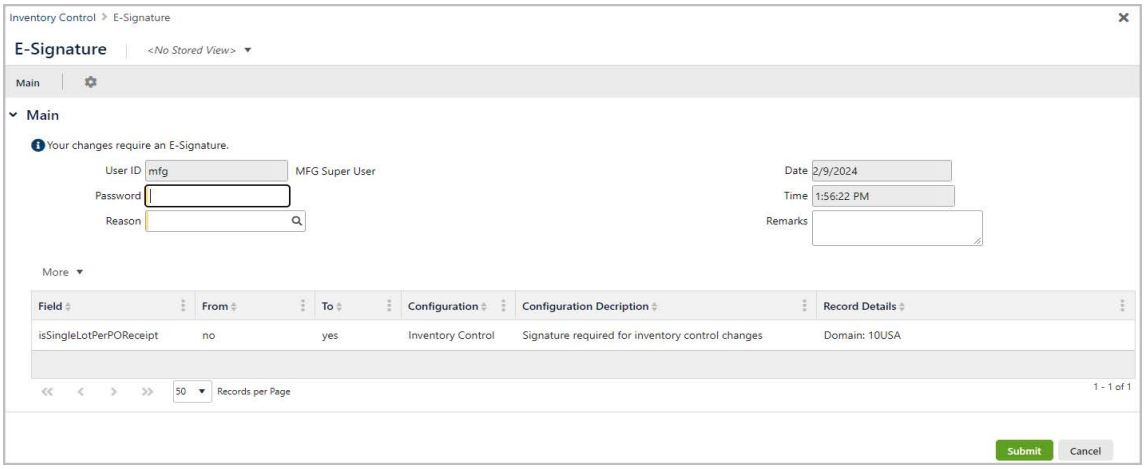
E-Signature Modes

In QAD Adaptive, you can use the e-signature functionality for the following types of business components:

- Previewable
- Non-Previewable

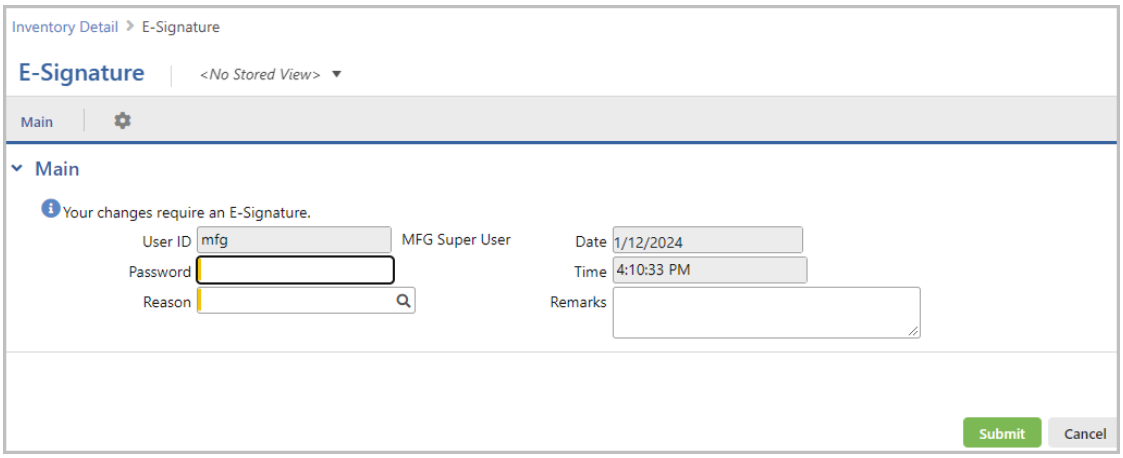
When signing changes in previewable business components, you can preview the field value changes in a separate e-signature pop-up before you sign and commit the transaction. The changed values are displayed in the From and To columns of the grid in a separate e-signature pop-up window, as shown in Figure 8.9.

Fig. 8.9
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 8.10.

Fig. 8.10
Inventory Detail, E-Signature Pop-up

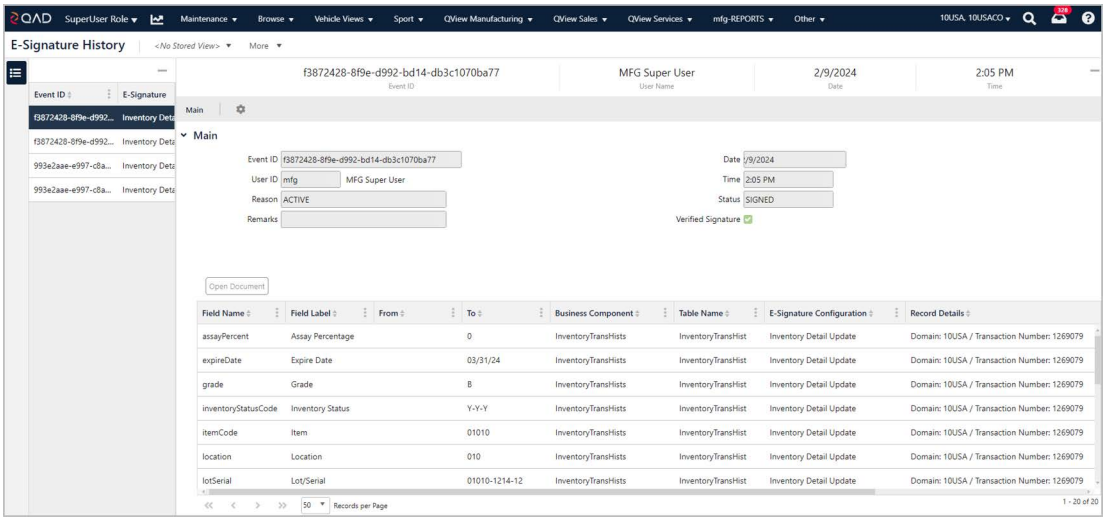


During an e-signature flow, the non-previewable business components use database sequences with the following technical limitation: sequence increments cannot be undone with a database transaction. This causes sequence gaps. Since you may not want to sign the changes and your operation may in fact be 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 8.11.

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. 8.11
E-Signature History

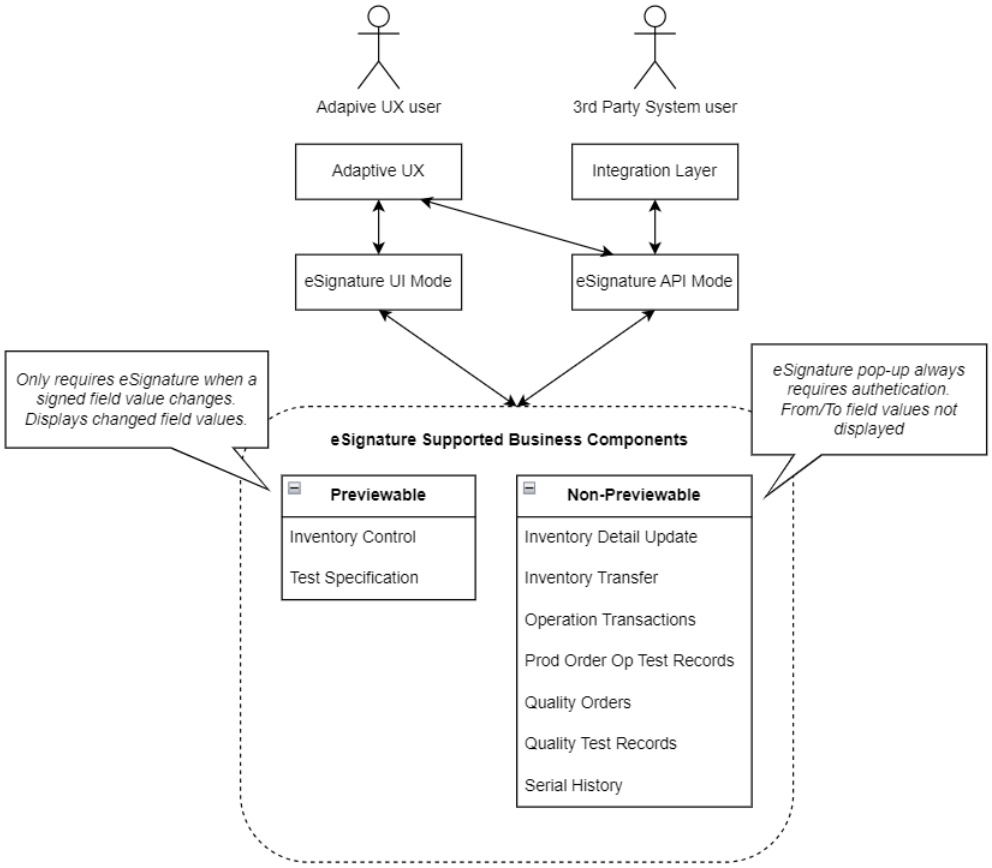


For both types of business components described above, you can use the following e-signature modes:

- E-Signature UI Mode
- E-Signature API Mode

Figure 8.12 shows the principle of user interaction with e-signature modes and different types of business components.

Fig. 8.12
User Interaction with E-Signature Modes and Business Components



E-Signature UI Mode

For e-signature UI mode, QAD Adaptive provides user interface dialogs for signing operations. This mode is used by users who directly enter data in QAD Adaptive.

E-Signature API Mode

For e-signature API Mode, QAD Adaptive 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 8.13 and Figure 8.14.

Fig. 8.13
Error for E-Signature with Field Value Changes Preview

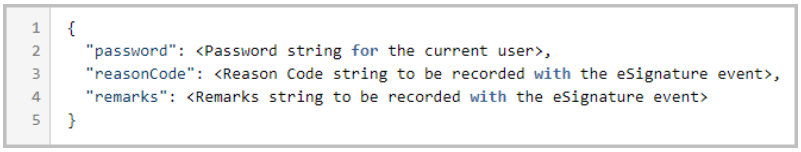
```
{
    "submitResult": {
        "errors": [
            {
                "severity": 1,
                "code": "0",
                "message": <variable base64 encoded value>,
                "fieldName": "",
                "messageType": "com.qad.qra.esig.ESignatureRequiredException",
                "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. 8.14
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. 8.15
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 8.16.

Fig. 8.16
E-Signature Token

```
{
    "submitResult": {
        "errors": [],
        "showResult": true,
        "resultMessage": "",
        "success": true,
        "errorSeverity": 0
    },
    "data": {
        "password": "",
        "reasonCode": "COMPLY",
        "remarks": "test",
        "token": "eyJhbGciIDogIkhTMjU2IiwidHlwIiA6ICJKV1QifQ.eyJleHAiOjE3MDY2OTc1OTEsImlhdCI6MTcwNjYxMzMzOSwiaXNzIjoidXJuOmNsaWVudGlkOm3iMTBmOTM3MzMxOTRhODFiYzE0NDQ1MTA4NGM0NzU5IiwiczViIjoidXJuOnNlc3Npb25pZDpBOTcwNjJjCQ
    }
}
```


The received token must be attached to the `X-QAD-Esig-Token` HTTP request header.

Index