QAD Enterprise Applications
Standard Edition

Training Guide

Security and Controls

70-3053A
QAD 2010 Standard Edition
Aug 2010

SecurityAndControls_TG_v2010SE.pdf/cxk/mdf

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

Contents

About This Course

Course Description

This course provides training on Security and Controls in QAD Enterprise Applications.

- Certification Preparation
- Other QAD Documentation
- Online Help
- QAD Website
- Conventions

We have provided a QAD on-demand environment to enhance QAD training guide materials. Please read these instructions to launch an environment to use with your QAD product training guide.

Course Objectives

By the end of this class, students will understand:

- QAD security and control capabilities
- Audit Trails concepts and configuration
- Electronic Signatures concepts and configuration
- Enhanced Security concepts and configuration

Audience

System administrators

Prerequisites

Basic knowledge of QAD Enterprise Applications Standard Edition

Course Credit and Scheduling

This course is valid for 6 credit hours.

This course is typically taught in one day.

QAD Web Resources

The QAD website provides product and company overviews. The Print Solution option on the opening page provides a means of compiling desired content into a document specialized to your industry, business implementation, and needs.

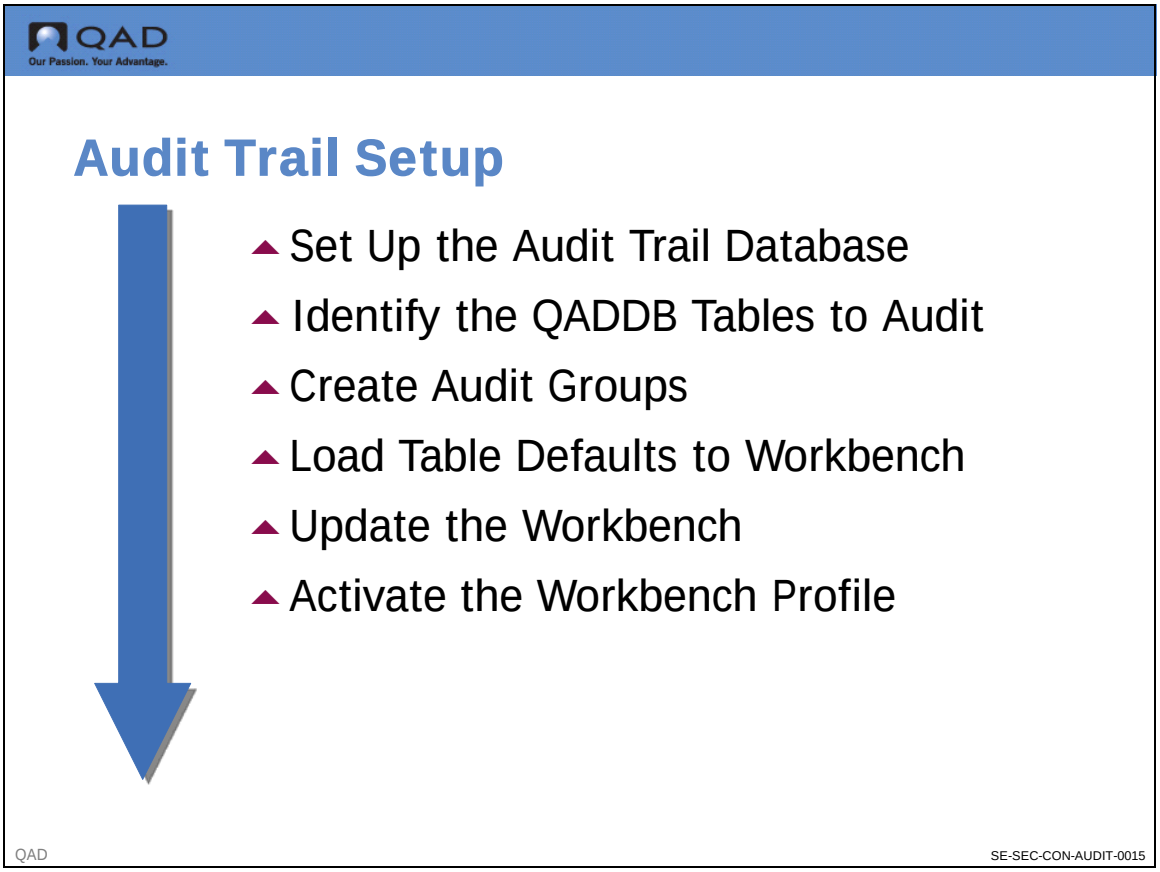
http://www.qad.com/

From QAD’s main site, you can access QAD’s Learning or Support sites.

Chapter 1

Audit Trail Basics

Audit Trail Setup



This chapter covers:

- User accountability basics
- Execute audit trail setup steps
- Administer audit trail creation process
- Run Audit Trail Reports for existing and deleted records
- Audit trail setup reports

User Accountability Basics

This section covers the following areas:

- Why are these features required?
- What is user accountability in QAD SE?
- Audit trail setup
- Audit trail administration
- Audit trail reporting

Why Do We Need User Accountability?

21 CFR Part 11 mandates the use of secure computer-generated time stamped audit trails to record user updates to electronic records.

21 CFR Part 11 does not mandate that you do this throughout your system. Selected areas around areas of GXP Compliance are the areas where people typically need audit trails enabled.

21 CFR Part 11 also allows for the replacement of handwritten signatures with signatures executed electronically.

This is the enabling part of 21 CFR Part 11. It gives regulated companies the opportunity to take handwritten signatures from their paper documentation system and to execute those signatures within software.

In addition to 21 CFR Part 11, other regulatory bodies also dictate the need for secure audit trails (and perhaps signatures). An example of this is Sarbanes-Oxley. Audit trails are a major underpinning to any Sarbanes-Oxley initiative.

What Is User Accountability In QAD Enterprise Applications?

There are two elements that address this.

The first element is audit trails. Audit trails record updates to QAD Enterprise Applications data in any or all tables in QADDB.

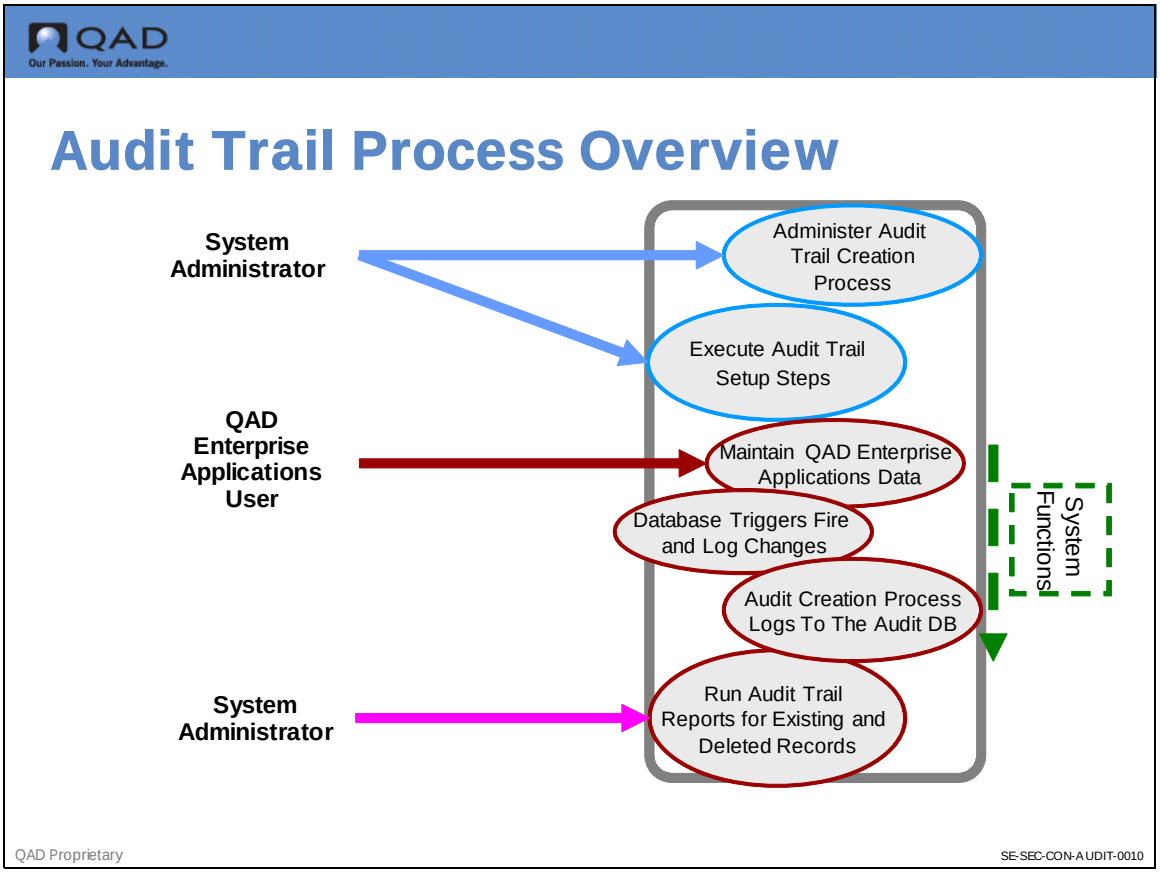
Note There are a number of identified tables that cannot be audit trailed, specifically those that concern security requirements.

Audit trails are based on triggers in the database schema and are independent of the process that activates them. Therefore, you do not have to be in the application to have audit trail triggers fire.

If the database is accessed through the Query Editor or other means, these audit trail triggers fire and log any changes to data that occur.

The second element of user accountability in QAD Enterprise Applications is electronic signatures. This allows, using user logon ID and password, a signoff of transactions performed in QAD Enterprise Applications.

Audit Trail Process Overview



Some functions for the audit trail process are system administrator driven (setting up the audit, setting up the tables to audit trail, and executing audit trail setup steps to enable those tables for audit trail).

As the user accesses the application, makes changes that impacts functions and implicate tables that are audit trail-enabled, automatically fires the database trigger.

The audit creation process then logs the activity to the audit database.

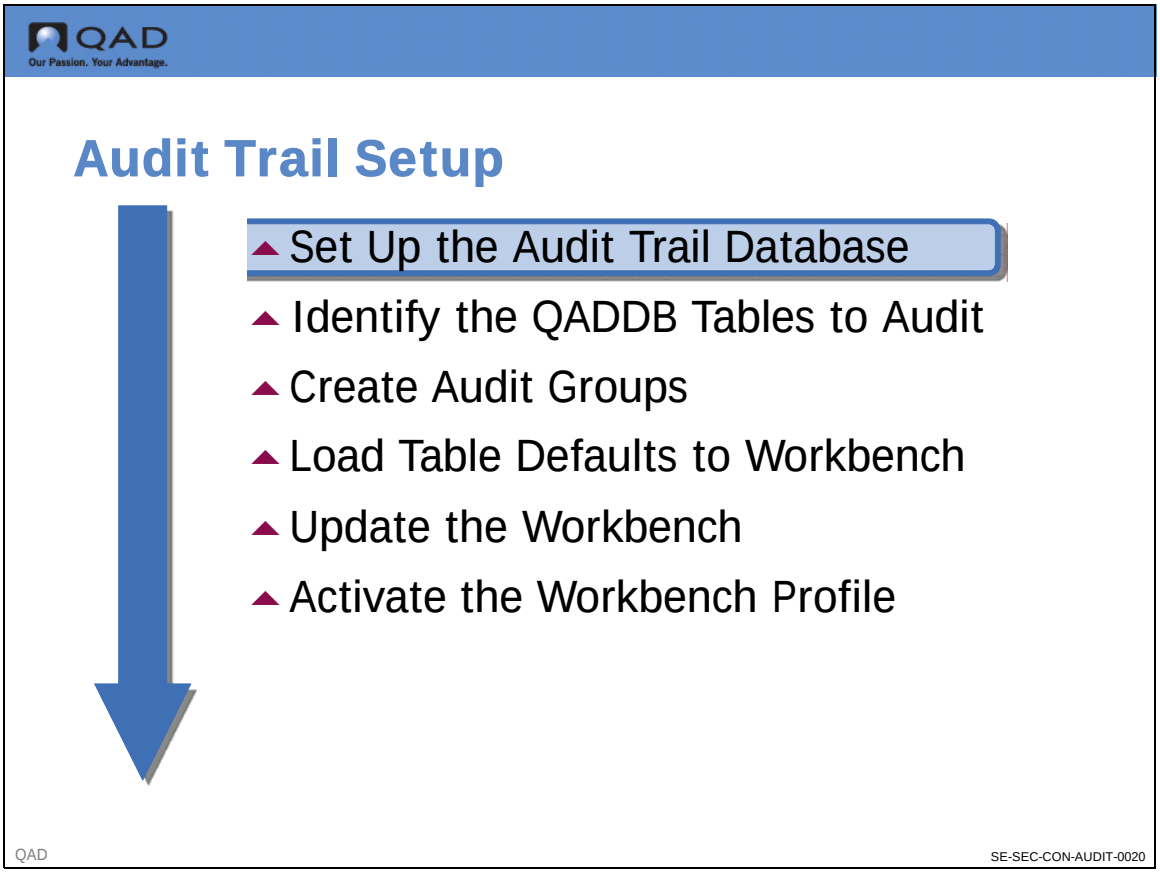
Once that finishes, audit trail data is available for the system administrator and Audit Trail reports can be run for existing and deleted records.

Execute Audit Trail Setup Steps

- Setup the audit trail database
  - Audit data is stored in a separate database, so you need to set up that audit trail database
- Identify the QADDB tables to audit trail-enable
  - Which tables in your particular application are required for Audit Trail? This may be related to regulatory requirements or an organization’s internal standard operating procedures.
- Associate those tables with audit groups
- Load table defaults to the workbench by audit group

- Update the workbench and identify any non-standard keys required for reporting deleted data
- Activate the workbench profile created

Set Up the Audit Trail Database



Why a use separate audit trail database?

The audit trail data is automatically archived to a separate database close to the time of generation. This design approach was adopted because of the considerable storage needs of audit trail data and the potential to exceed Progress data storage limits within a single database.

In a separate audit trail database you can maintain multiple audit trail databases and bring new audit trail databases on-line when a audit trail database fills up.

Audit Trail Database Setup

Audit trail database setup consists of the following steps.

First, you need to set up an audit trail database through the QAD Enterprise Applications (MFG/UTIL) function, (see the QAD SE Installation Guide for details on this step).

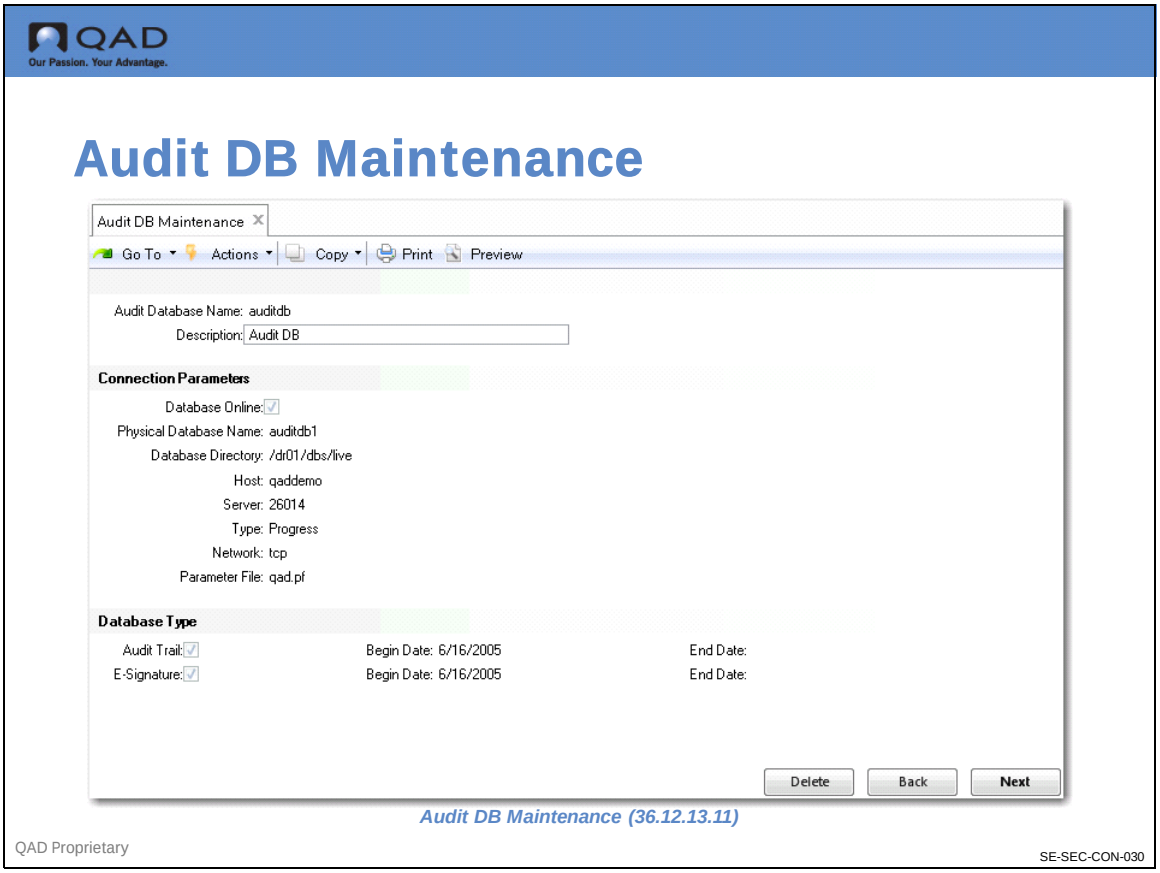
Next, start the audit trail database servers.

The final step is to identify the Audit Trail database name and connection parameters through the Audit Database Maintenance (36.12.13.11) function.

This function enables you to identify the audit trail databases available on your system, which is the current one, and how to access that database.

On the screen you identify an audit database name, which is a unique identifier for the database. This is not the physical database name it is only an identifier for the database.You provide the description.

Audit DB Maintenance (36.12.13.11)



Audit DB Maintenance (36.12.13.11)

Audit Database Maintenance (36.12.13.11) Identification Fields

Audit DB Name. A unique QAD SE identifier for this database

Description. Enter a description

Begin Date. The date this database comes on-line and become the current audit database. No two audit databases can have the same begin date.

End Date. Automatically filled by the audit trail creation process as it brings a new audit DB on line.

There is a flag identified on the screen called Database Online.

Connection Parameters Non-Progress

Database Online is a manual identification of whether the database should be currently available. It should be set to No if the database was removed from the system or if the servers are not normally active for that database.

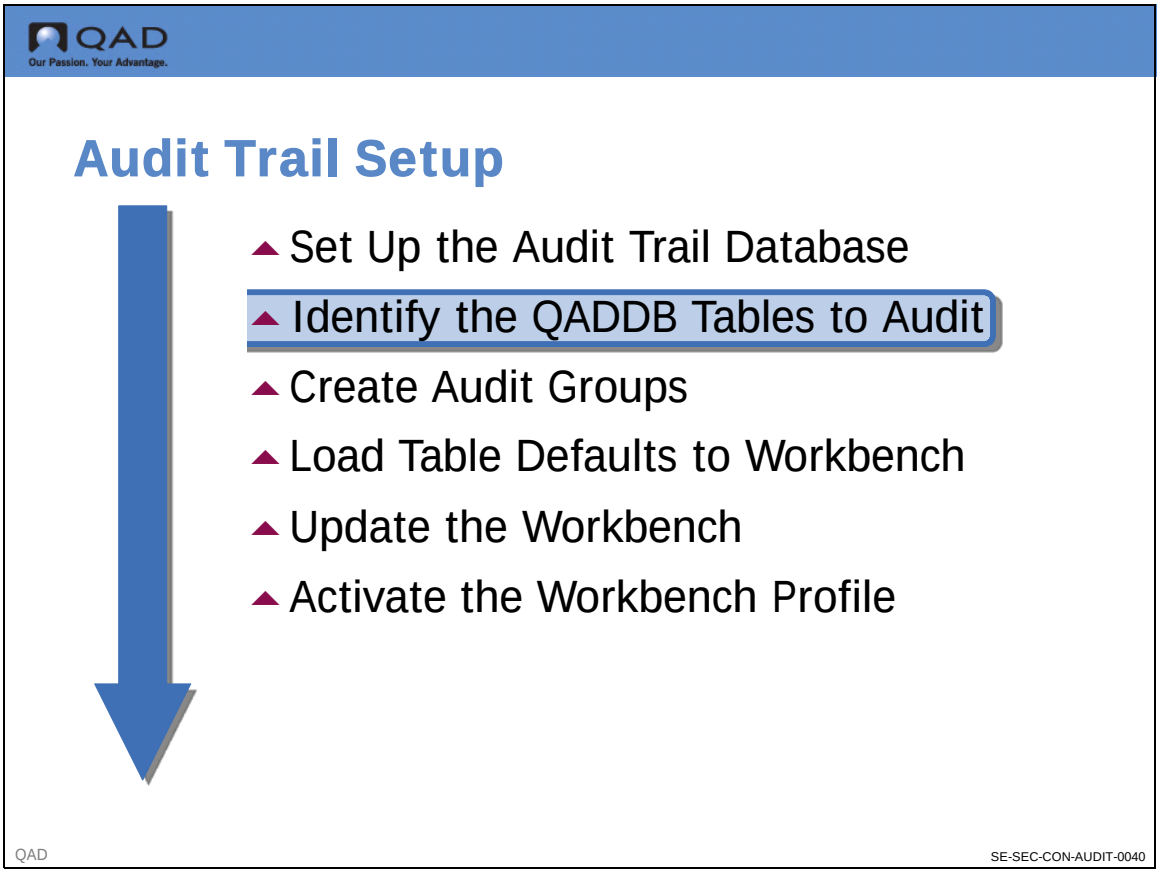
Database Online was implemented to avoid attempts by the audit trail reports to open databases that are referenced in Audit DB Maintenance (36.12.13.11) but are no longer available.

Note This flag does not indicate whether the database can be connected to. It is not a check that the system is running against the database to ensure it is alive and available.

Connection Parameters Progress Related

The rest of the parameters are Progress-related and are required by the needs of Progress to connect to another database. They relate to what type of a connection to attempt to establish with the database, what the host name is, and what the server name is. These parameters are the same as those identified in Database Connection Maintenance (36.6.1). Refer to the Progress documentation for further details regarding these parameters.

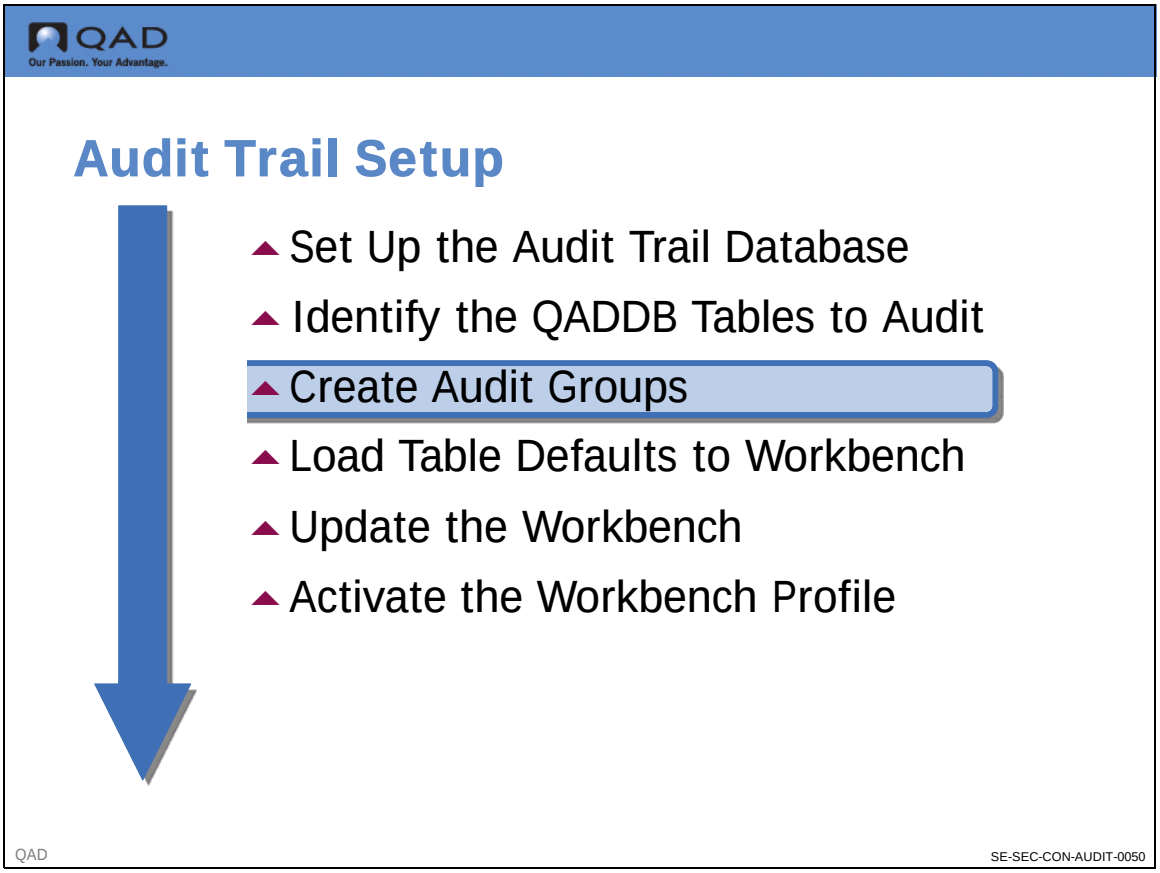
Identify the QADDB Tables to Audit



QAD recommends that you use the entity diagrams and the database definitions reference guides to assist in identifying the tables associated with menu functions and processes in QAD SE.

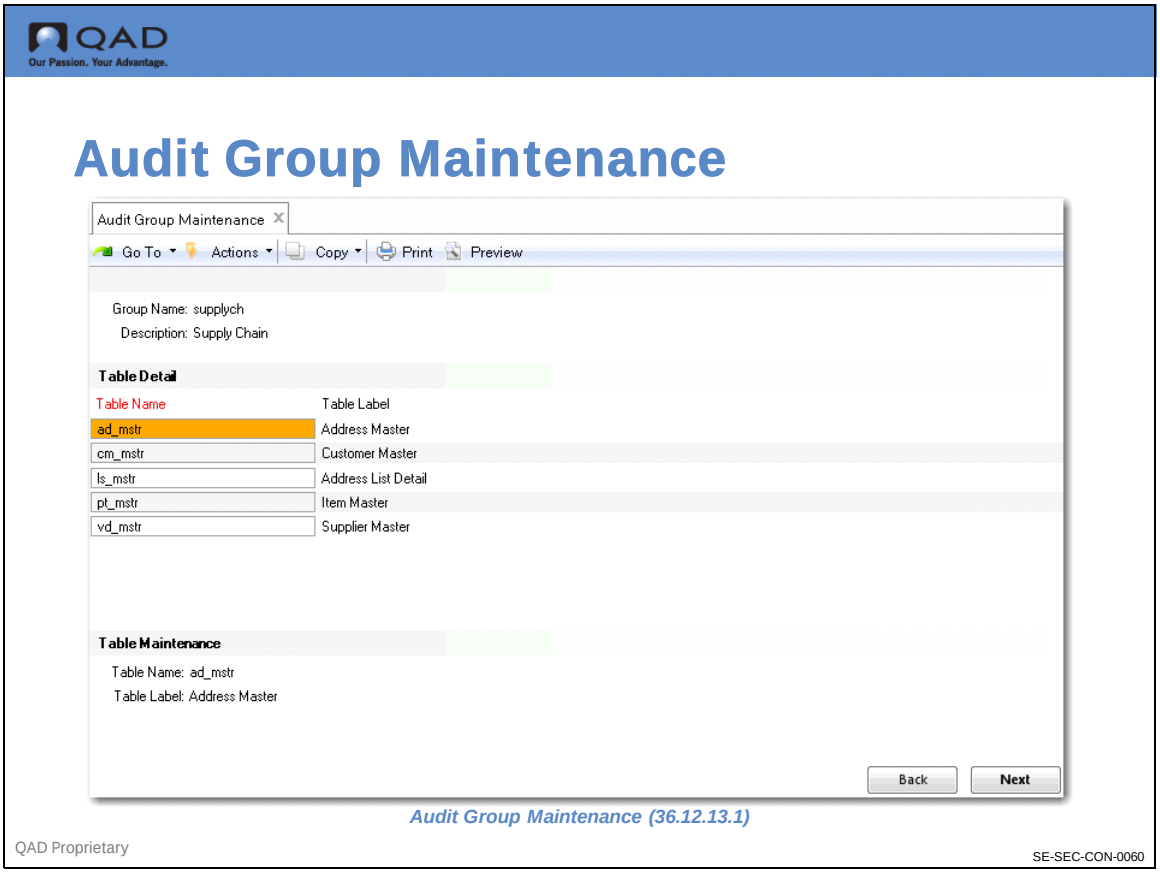
Use the entity diagram information to identify database tables associated with particular functional areas of the system and the database definitions to identify the field level detail, especially in terms of delete keys.

Create Audit Groups



Audit groups are optional, but they simplify the task of managing the tables in the workbench and when activating a profile. For this reason QAD recommends that you use audit groups to manage groups of tables. Refer to the Audit Group Maintenance (36.12.13.1) screen.

Audit Group Maintenance (36.12.13.1)



Audit Group Maintenance (36.12.13.1)

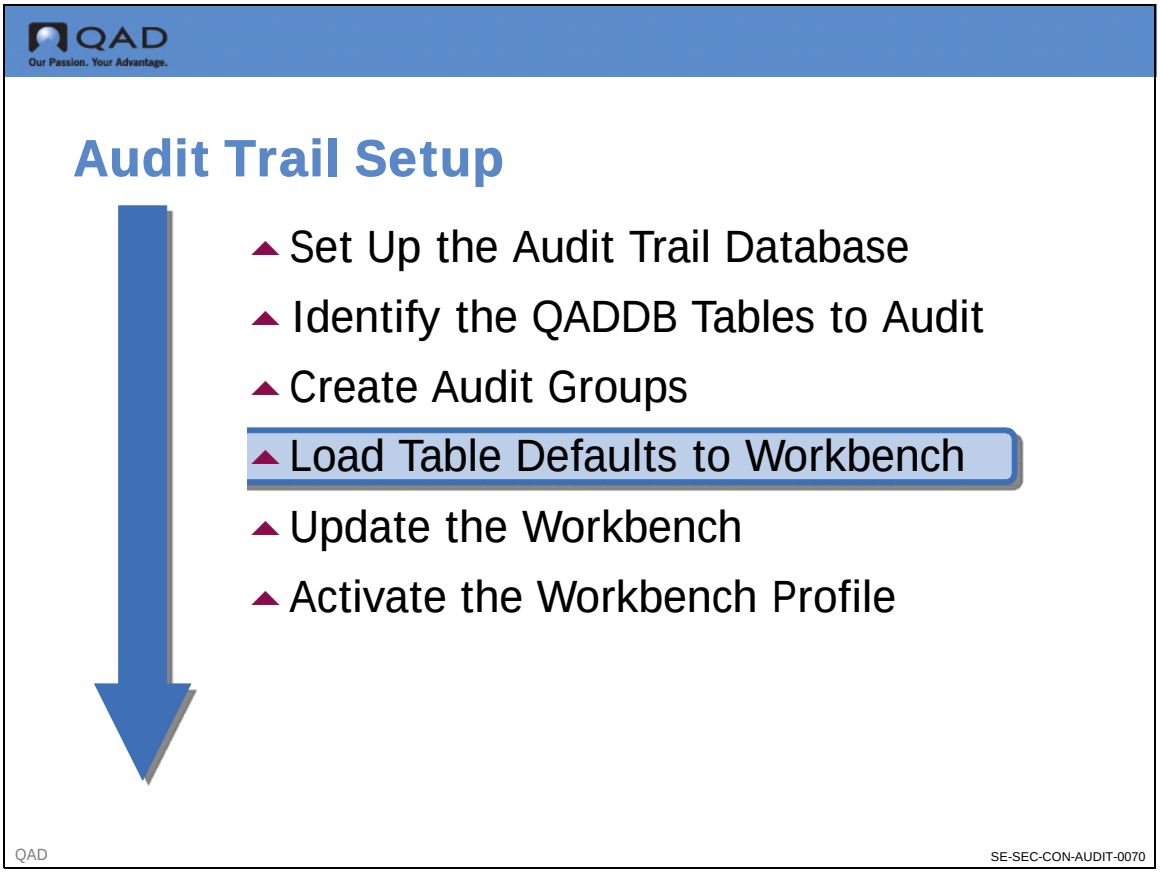
Group Name. Use the name of a functional area such as Supply Chain or Shop Floor to control the tables.

Description. Enter a freeform text description.

Table Name. Name of the QAD Enterprise Applications table to add to this Group.

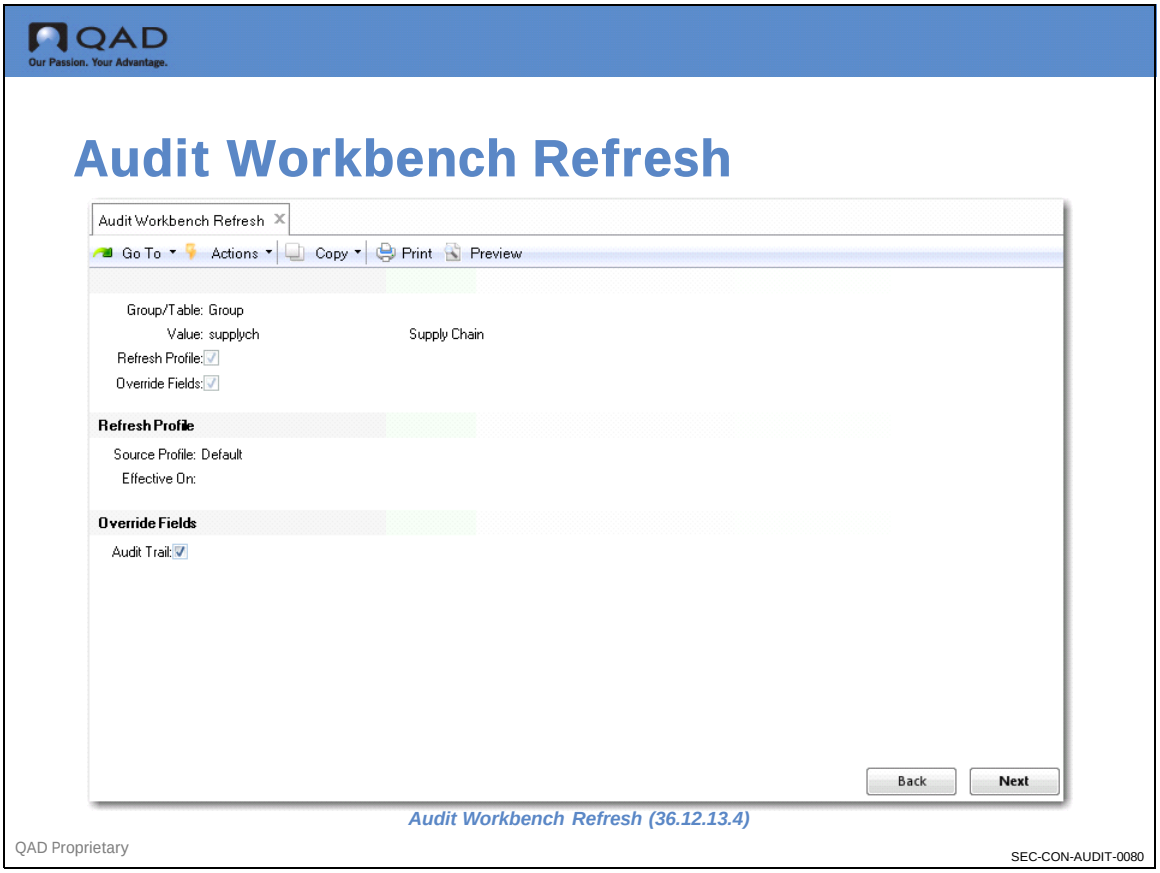
The Audit Group Maintenance (36.12.13.1) screen allows you to identify a Group Name, Description, and basic table details.

Load Table Defaults to Workbench



The next step is to load the table defaults to a workbench function from within which you can convert your particular configuration into a profile to have active and live.

Audit Workbench Refresh (36.12.13.4)



Audit Workbench Refresh (36.12.13.4)

Audit Workbench Refresh (36.12.13.4) loads individual tables, table profiles or a group of table profiles to the workbench. Profiles can be loaded from the default table profiles supplied by QAD or from profiles that you already have activated.

From this screen you can specify whether to load from an actual group, load the tables relevant to a particular group, or just load an individual table into the workbench.

Group/Table. Select a single table name or an audit group name to load from.

Value. The table or group name.

Refresh Profile. Indicates whether profiles currently in the workbench should be refreshed using default or active profile data.

Override Fields. If set yes, allows the user to set the default value for the Audit Trail Y/N flag for all tables selected by the Refresh function. If Refresh Profiles is set to No, this only applies to profiles currently in the workbench.

Source Profile. Specify Default for the QAD supplied default table profiles or Active to load activated profiles back to the workbench for refinement.

Effective On. The profile is refreshed using the profile settings active for the table or group of tables on the nominated date. If any of the source table profiles were not active on the date, tan error message are generated. This value is not prompted for when Source Profile is set to default.

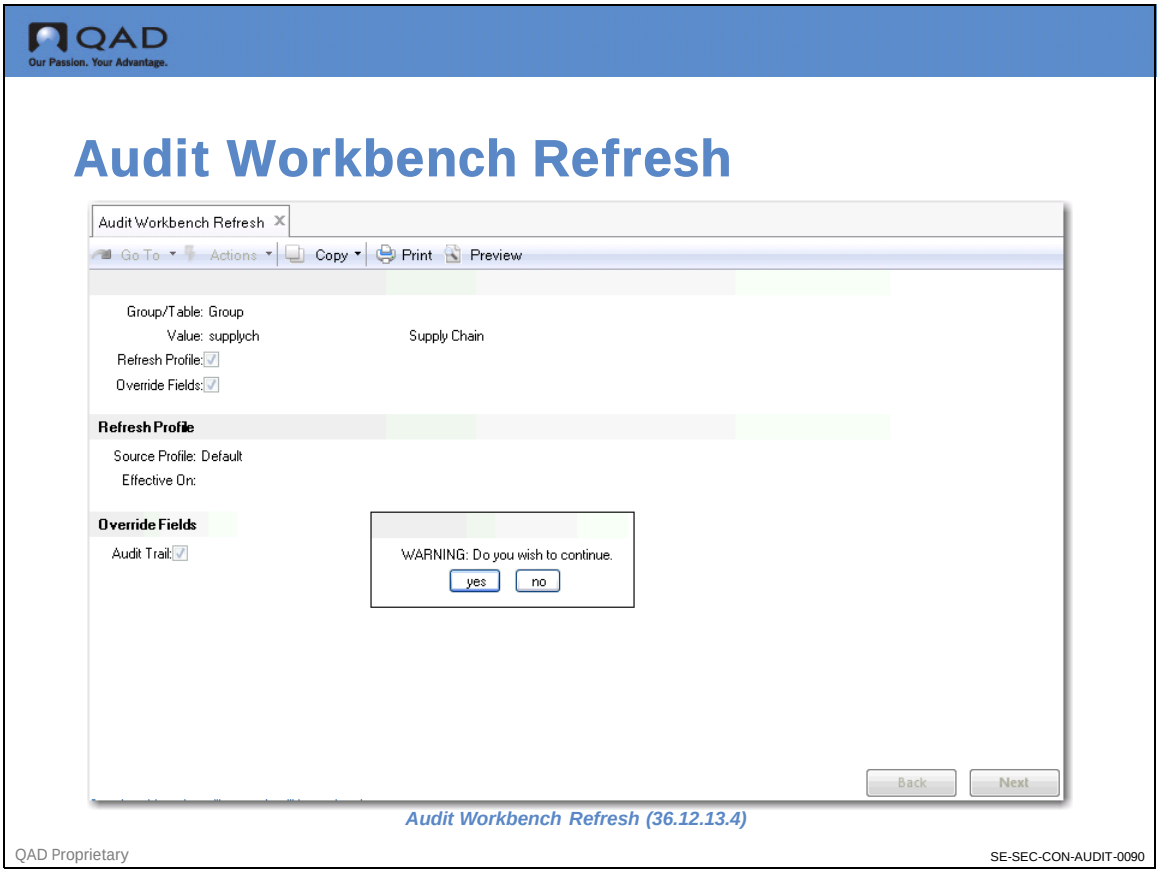
Audit Trail. The Audit Trail yes/no field for any table profile selected by the refresh defaults to the value entered here.

If you load a group of tables into the workbench, and set this field to Yes, all of the tables load into the workbench as Enable Audit Trails.

If you set it to No, it is disabled for all of the tables. This is an important feature because there is no way to delete any profile that has been activated.

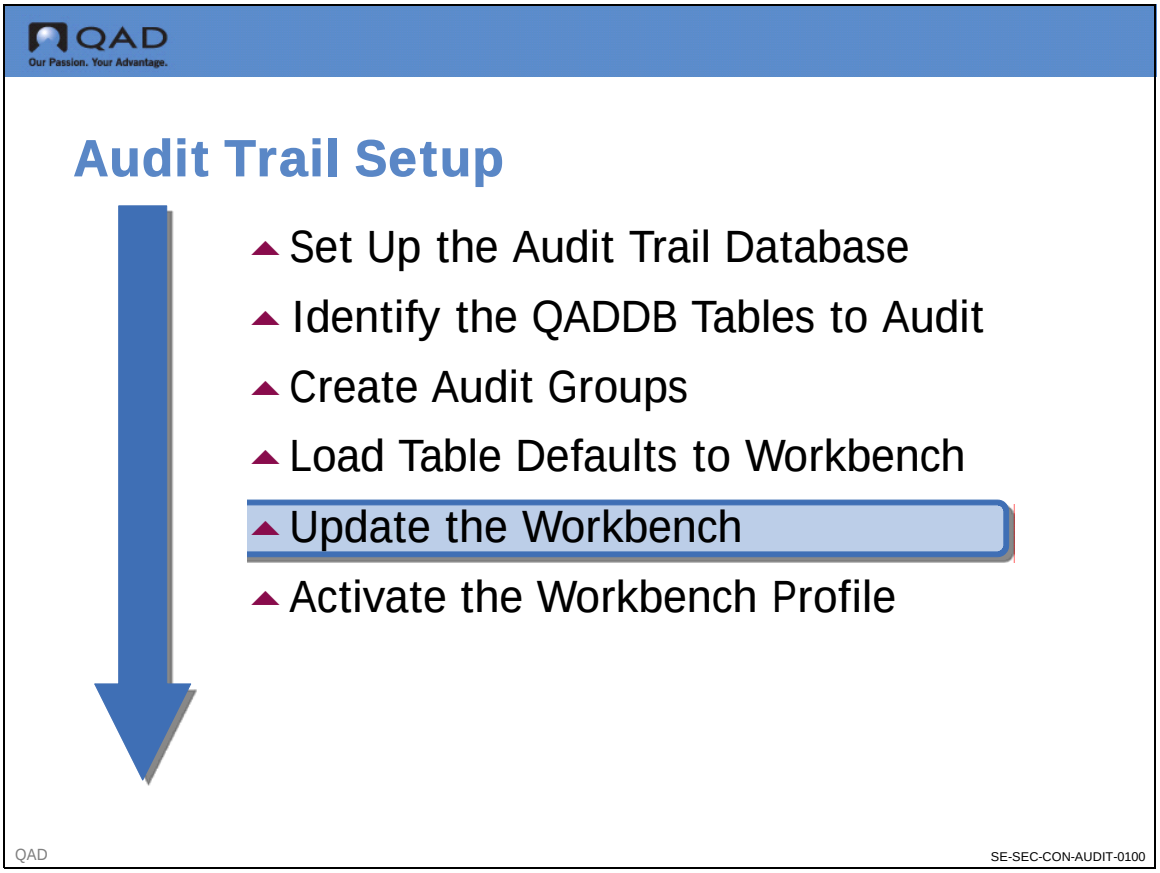
The only way to turn off Audit Trails for a table is to create a new active profile that switches off Audit Trails for that table.

Audit Workbench Refresh (36.12.13.4)



Audit Workbench Refresh (36.12.13.4)

Update the Workbench



Audit Workbench Profile Maintenance

The Audit Workbench Profile Maintenance (36.12.13.5) allows for the customization of audit trail operation by table. It serves two primary purposes:

- To indicate if audit trails are enabled or disabled for a particular table
- Allow for the definition of delete event keys

Audit Trails

When you install there is no active profile for any table, i.e. audit trails are disabled for all tables. Once an active profile has been created for a table, the only way to modify the profile is to create a new profile for the table that overrides the condition that existed in the previous profile.

Therefore, the only way to cease audit trails in the table with an active profile, is to create an active profile for the table, this disables auditing.

Delete Event Keys

For audited data that has not been deleted, the audit trail reports locate the audit trail by first finding the audited record followed by the audit data. In this way, any fields present on the audited data can be used to select the data.

Once the subject data has been deleted, this can no longer occur. Deleted audit trail reports can only locate data by going directly to the audit trail.

By default, only the primary index fields are stored with the audited data in a form that allows them to be used as selection criteria. In order to have fields other than the fields of the primary index stored with the audited data, delete event keys must be defined in the workbench for those fields. These keys are not required for audit data that has not been deleted.

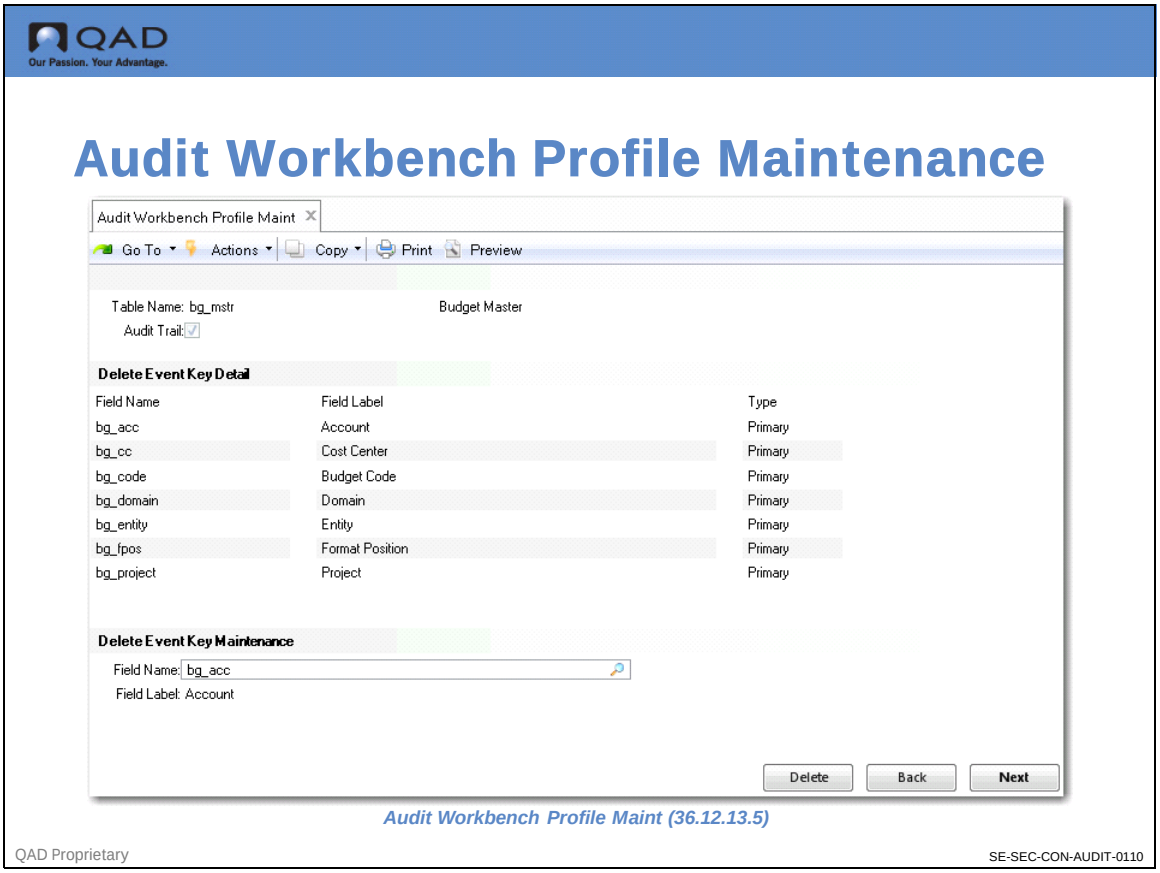
By default, only the primary index fields are stored with the audit data in a form that allows them to be used as selection criteria. They are separated out from the actual audit trail data and can be used as selection criteria.

To have fields other than those of the primary index stored with the audit data, delete event keys must be defined in the workbench for those fields.

For example,

- For a sales order (so_mstr), once the sales order is deleted, the only way to locate the audit trail data would be to search by sales order number (so_nbr).
- If search was more commonly performed by customer, customer number (so_cust) would need to be identified as a delete event key.
- For a sales order, so_mstr, once the sales order is deleted, the only way to locate the Audit Trail data would be to search by sales order number, because this is the primary index of so_mstr.
- If search was more commonly performed by customer, the customer number, so_cust, would need to be identified as one of these delete event keys.

Audit Workbench Profile Maintenance (36.12.13.5)



Audit Workbench Profile Maint (36.12.13.5)

On the Audit Workbench Profile Maintenance (36.12.13.5) screen you can identify these delete event keys. These are selected from the table in a straightforward manner.

In the maintenance fields on this screen, you have the name of a table currently in the workbench. Note that you cannot add tables to the workbench from Audit Workbench Profile Maintenance. The only way you can add tables to the workbench is through the refresh function.

This screen has the following features:

Table Name. The name of a table currently in the workbench. Tables cannot be added to the workbench here. Only workbench refresh can add tables.

Audit Trail. Indicates if audit trail is enabled or disabled for the table.

Delete Event Key Detail. Field Name: The field name.

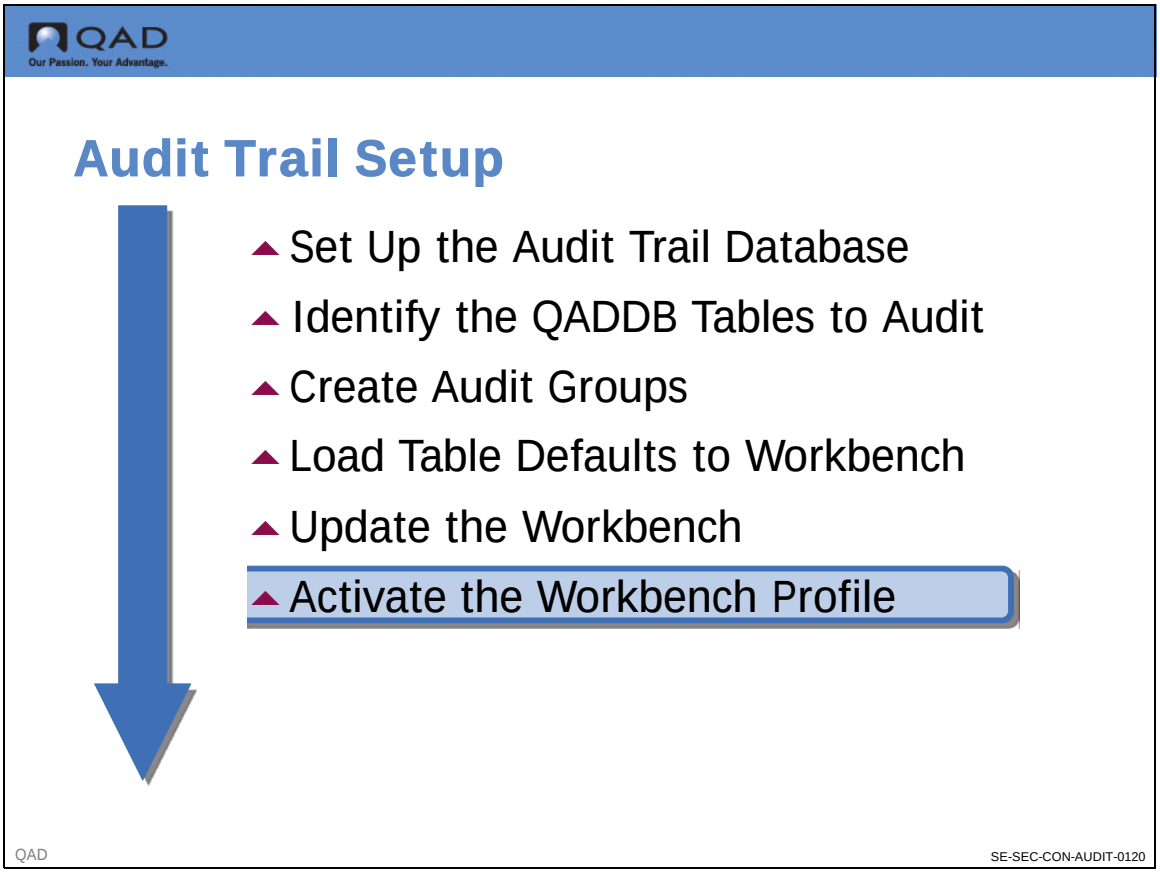
Field Label: The field label.

Type: Primary indicates that the field forms part of the primary index for the table. Primary types cannot be removed from the profile.

Other indicates a delete event key added by the user through the workbench. These can be added or removed from the profile.

The final phase is activating the workbench profile. Audit Profile Activation (36.12.13.8) takes the table or group of table profiles from the workbench and creates an activated profile.

Activate the Workbench Profile

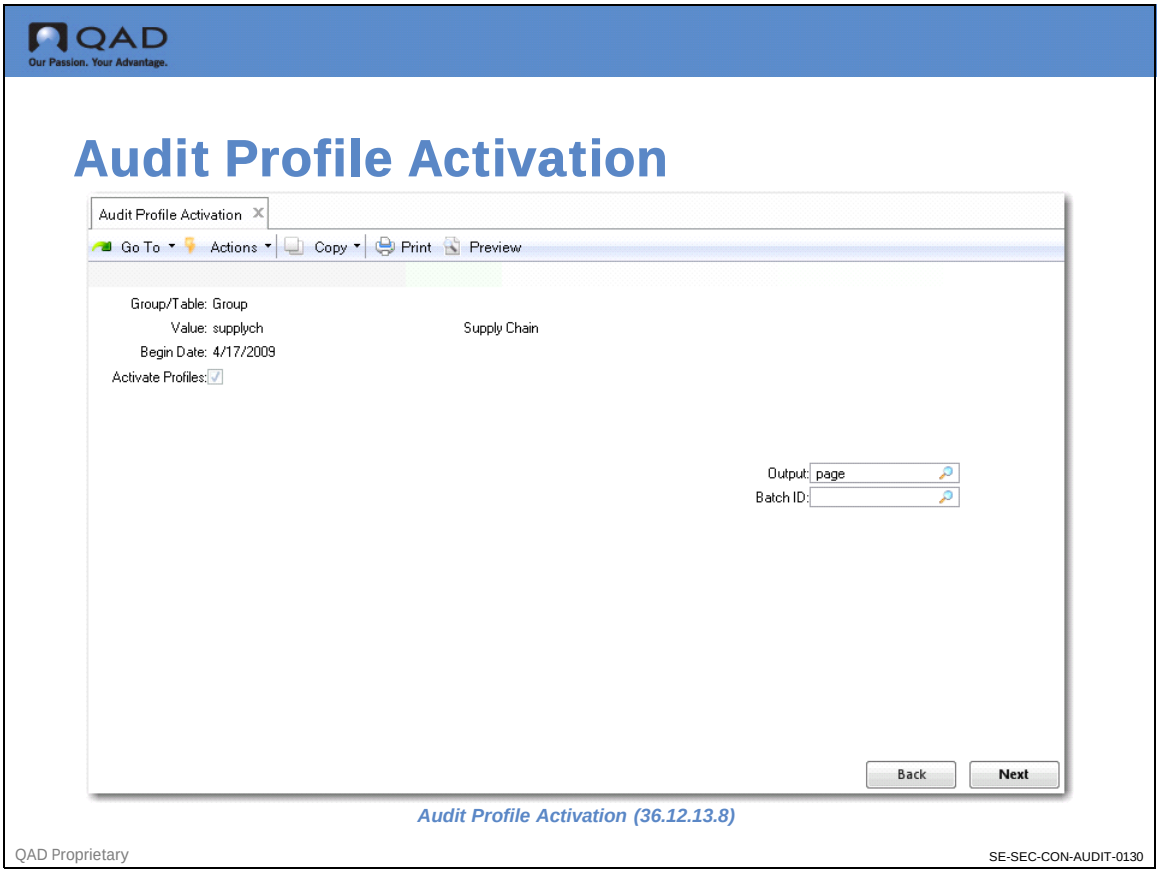


Audit Profile Activation

- Takes the table or group of table profiles from the workbench an creates an activated profile
- Profile activation takes place at 12:00 a.m. on the day nominated.
- As added security, an e-mail notification will be generated to members of the admin group identifying that a change has occurred to the active profile. The admin group is identified on the Security Control file and is a regular group within QAD SE.

  For e-mail notifications to work, users identified in the admin group must have an e-mail system set up, and they must have their e-mail address logged against their user information.

Audit Profile Activation (36.12.13.8)



Audit Profile Activation (36.12.13.8)

Group/Table. You can activate the profile by group or table. You can activate a profile for a single table or for one of the groups that you have identified.

Value. The group or table name.

Begin Date. The date when this profile becomes effective. Begin date must always be greater than the date that Audit Profile Activation (36.12.13.8) is run. If you run Audit Profile Activation (36.12.13.8) now, the earliest begin date you can set is tomorrow. This guarantees that there are no integrity issues in the changeover from one profile to the next.

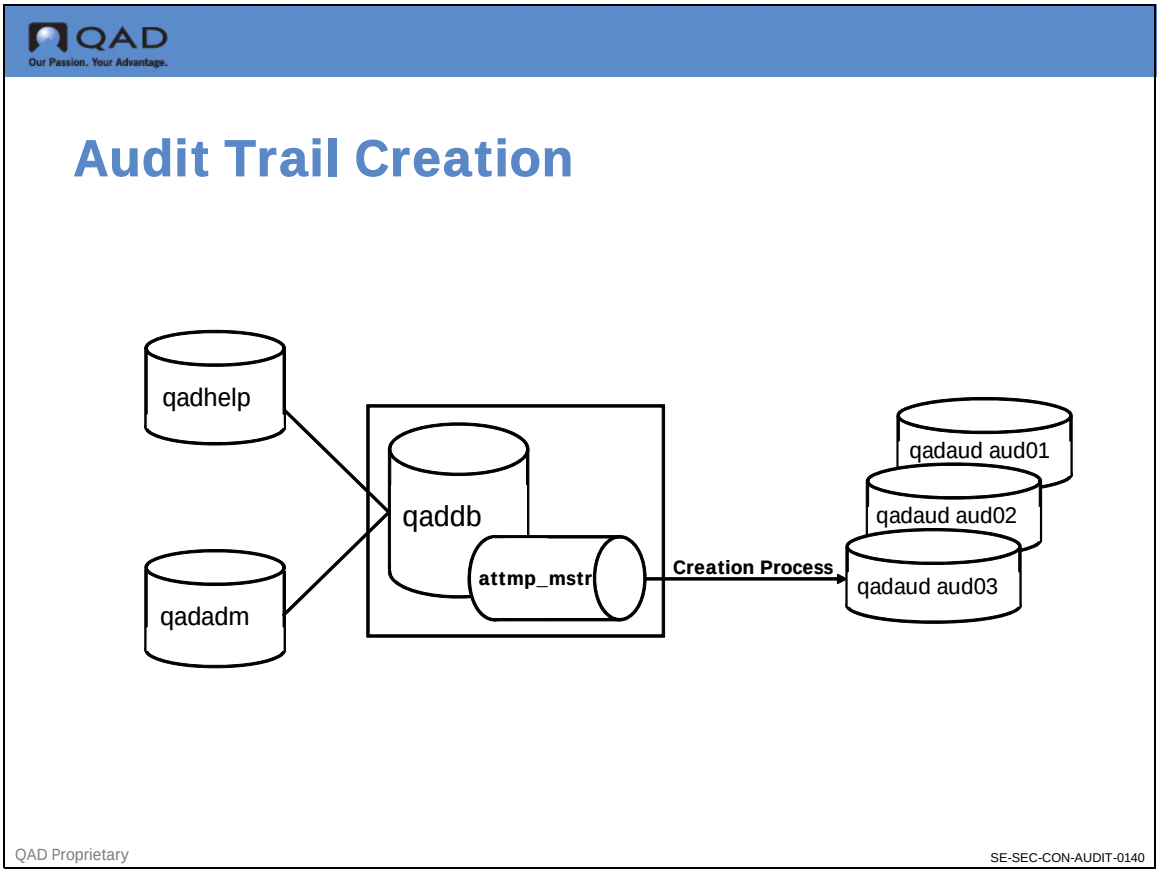
Activate Profiles. Answer No to only print a report of what profiles are activated if you had said Yes to Activate Profiles. That is a good check to see what you are trying to activate.

What active profile was in effect when this data was audit trailed? It might be problematic to determine to the minute when the profile was activated. It is much easier to always activate profiles at 12:00 a.m.

Administer Audit Trail Creation Process

After you have set up audit trails and identified the tables to audit. You go through the Administer Audit Trail Creation Process (36.12.13.23).

Audit Trail Creation



Because of performance considerations, audit data is created as a multi-step process. First, the audit data is written to a staging table in QADDB. Once the data is in the staging table, an audit trail creation process takes the data and archives it to the audit database, where it is permanently stored.

Final Audit Trail Creation Steps

- User updates data in an audited table
- Database trigger fires and the audit data is written to a table in QADDB called attmp_mstr
- Audit creation process takes data from attmp_mstr and archives it to the current audit database (qadaud)

  Remark. This is a freeform comment to associate with this use.

  Active. This flag indicates whether the user is active or not. Inactive user accounts cannot be used to log on to the system. If a user exceeds the maximum allowable logon attempts, this flag is automatically set to No.

  Active Reason. Whenever a users active status changes, a reason code must be assigned. For system initiated changes to a users active status, the reason code identified in the Security Control file is used.

Force Password Change. This flag enables the administrator to manually age a user's password. This condition is always true for newly created accounts or where the system administrator has assigned a new password to an existing account.

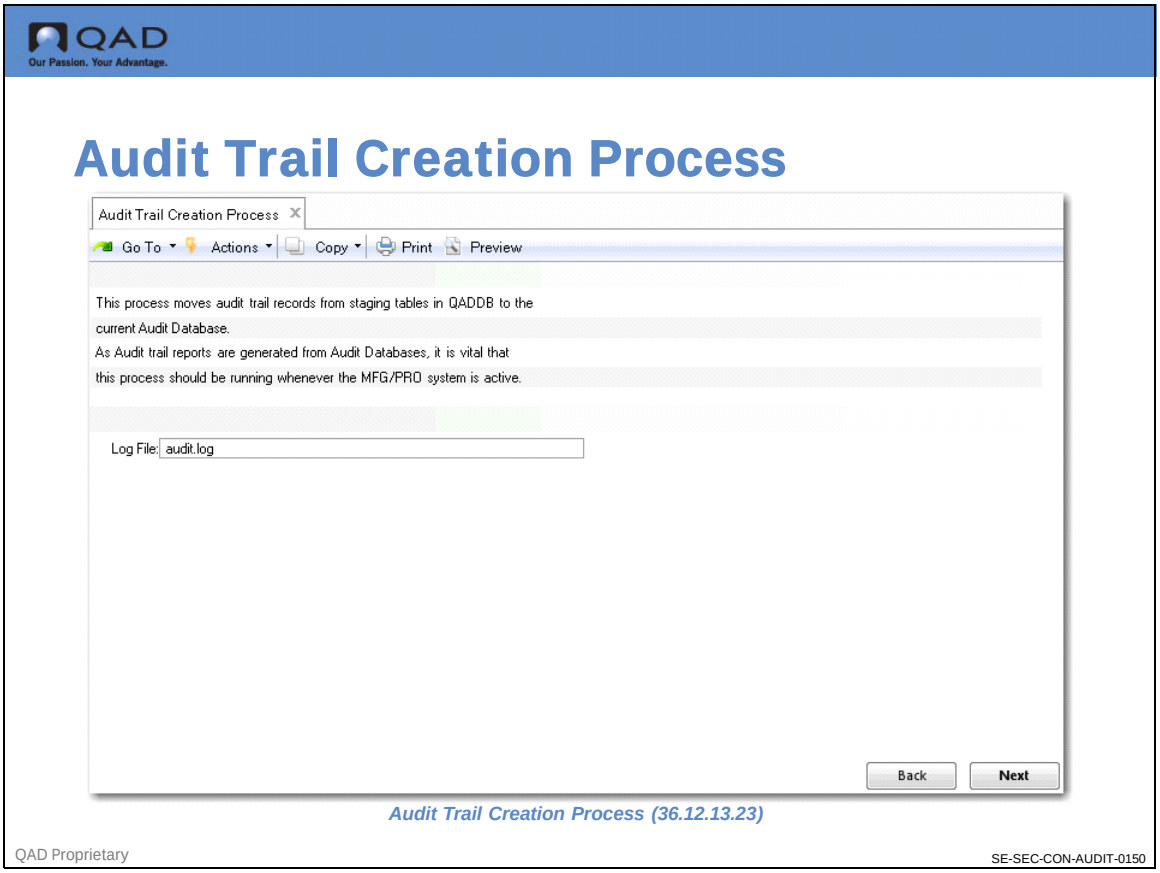
Last Logon. This field holds the last successful logon date and time for the user

Update Password. If set to Yes the user navigates to the password creation screen or automatically generates a new password. The behavior is driven by the password creation method parameter in the Security Control file.

The audit creation process operates as a separate distinct process, takes that data from the attmp_mstr table, and it archives it to the current audit database, the QADAUD database.

Some important features of the Audit Trail Creation Process (36.12.13.23) to remember is that audit Trail Reports take their data from the audit database, not the staging table, the attmp_mstr. Therefore, it is critical that the Audit Trail Creation Process (36.12.13.23) is always running whenever the database is active.

Audit Trail Creation Process (36.12.13.23)



Audit Trail Creation Process (36.12.13.23)

Audit trail reports take their data from the audit database, not the staging table (attmp_mstr). Therefore it is critical that the Audit Trail Creation Process (36.12.13.23) is always running whenever the database is active.

Audit Trail events can accumulate in the attmp_mstr if the Audit Trail Creation Process (36.12.13.23) goes down or is not live for any reason or period of time.

But the main limitation is that any audit trail reports generated while that process is down do not show up-to-date information. So the Audit Trail Creation Process (36.12.13.23) can be run:

- Multiple times for multi-threaded operation
- From the QAD Enterprise Applications menu or as a task in background

Audit Trail Creation Process can be started and left active for the day. From this screen you can identify a log file; it is actually an operating system file.

Log File. Processing errors that may occur as a result of the creation process are logged to this operating system file. The value of file name defaults from the user accountability control file.

Processing errors that may occur as a result of the creation process are logged to this file. The value of the file name is defaulted from the User Accountability Control file, but you can modify it on a session-by-session basis.

Shutting Down The Audit Trail Creation Process

The Audit Trail Creation process can be shut down from the User Accountability Control file. The User Accountability Control file has flag at the top that says AT Creation Process Shut Down Request.

User Accountability Control fields:

AT Creation Process Shutdown Request. Yes shuts down all AT creation processes. This is important because you can run multiple AT Creation processes.

Log File. The default value for the log file name entered when starting the AT creation process

Run Audit Trail Reports for Existing And Deleted Records

You might want to run audit trail reports for existing data on the system or for data you may have deleted from the system.

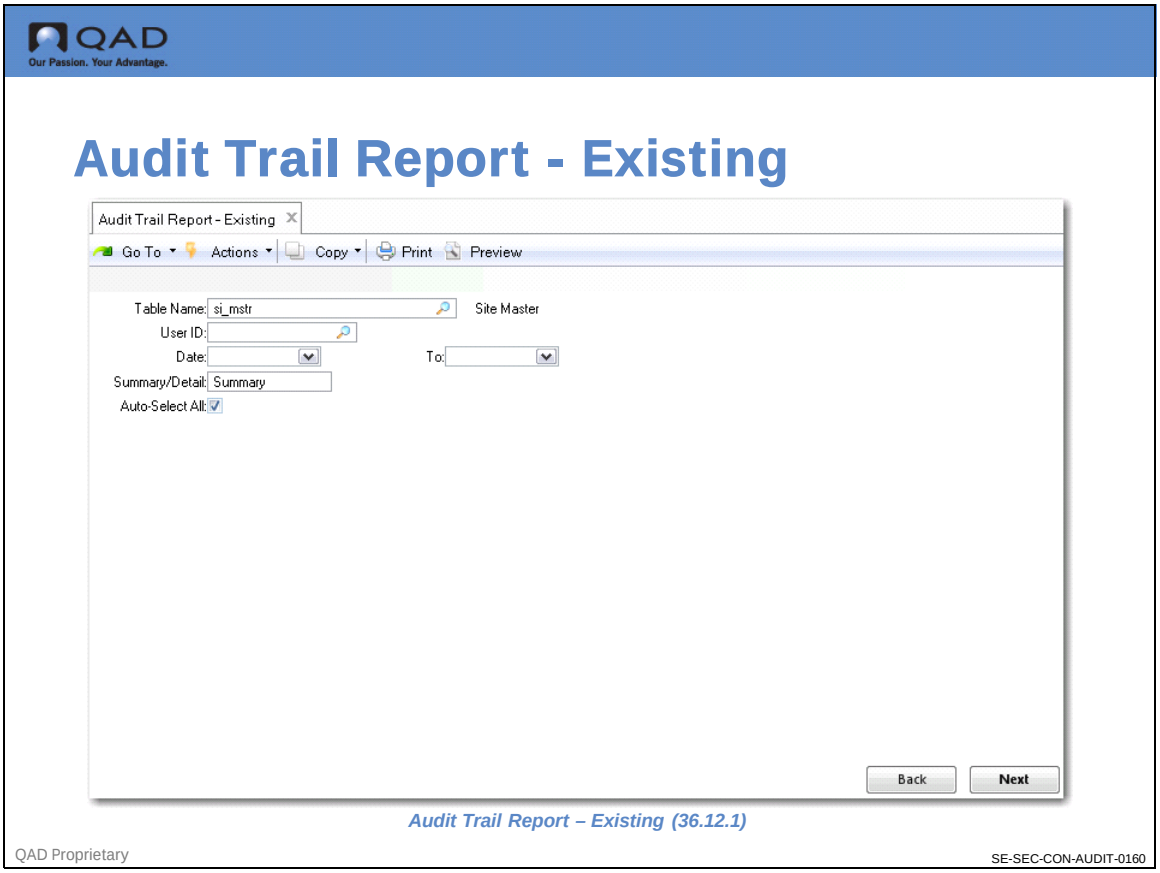
- Existing e-records
- Deleted e-records

Audit Trail Report Existing E-Records

Audit Trail Report Existing (36.12.1) allows for the selection of a range of records for a particular Audit Trail table and for the selection by any field in that table (any field in the subject record).

Using pt-mstr as an example, any field in pt-mstr can be used to select the primary pt-mstr record. From that record you can drill down to the particular audit trail events that relate to that particular record.

Audit Trail Report - Existing (36.12.1)



Audit Trail Report – Existing (36.12.1)

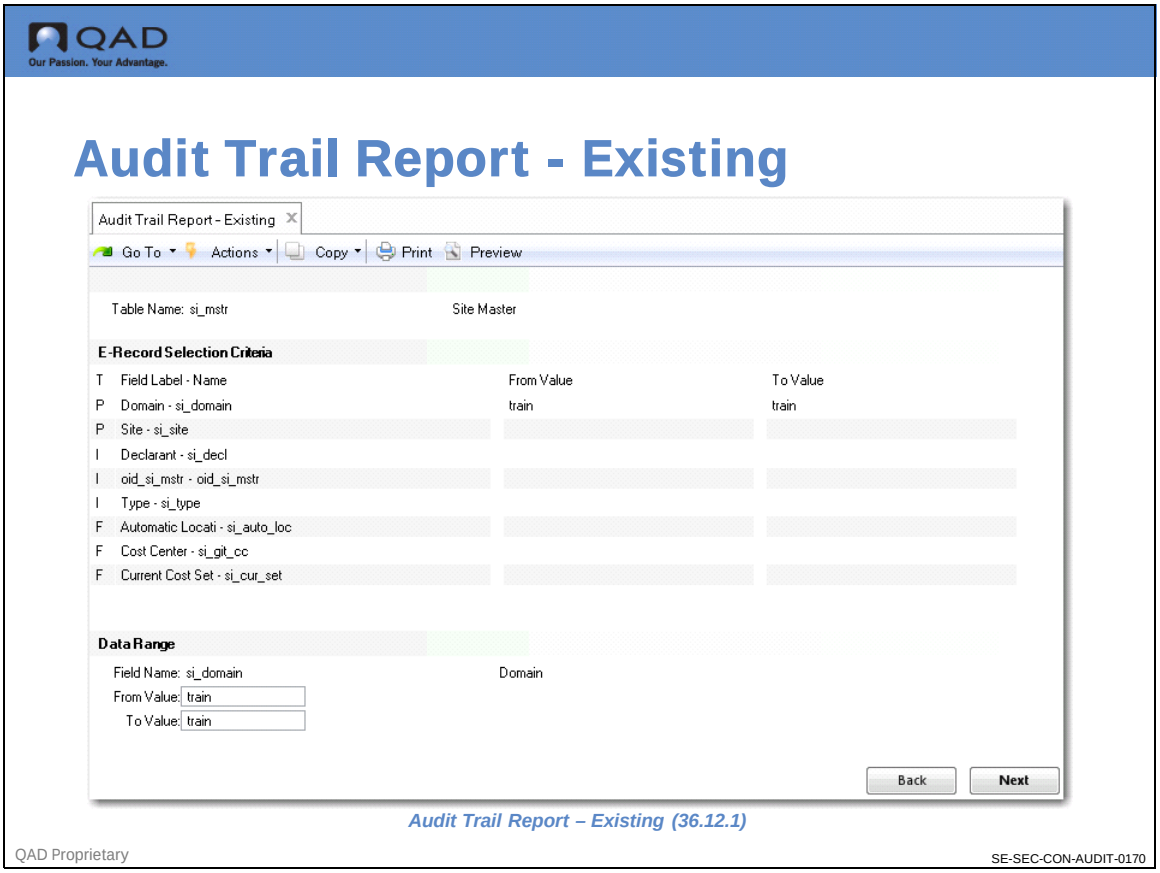
Because they are generic, they have a number of frame levels that you must navigate through to specify the necessary information to operate the report.

For the Existing E-Record Report, identify the table name and optionally a user ID of the person who performed the update. You can also enter a date range for the audit trail events and also whether to display summary or detail information.

There is a flag called Auto Select All. In a subsequent frame it allows the user to select the fields to display on the report (these are the fields that will display, these are not the fields to use to filter the data). Setting this to Yes, indicates that on this subsequent frame all of the fields will be selected by default while No indicates that no fields will be selected by default.

Once you enter the frame, you can modify those defaults to be Yes or No based on whether you wish to identify those particular fields.

Audit Trail Report Existing E-Records Frame 2



Audit Trail Report - Existing (36.12.1)

In the E-Record Selection Criteria frame, you are offered all the fields in the table that you have identified. You can identify From and To ranges. This is the filtering for the report.

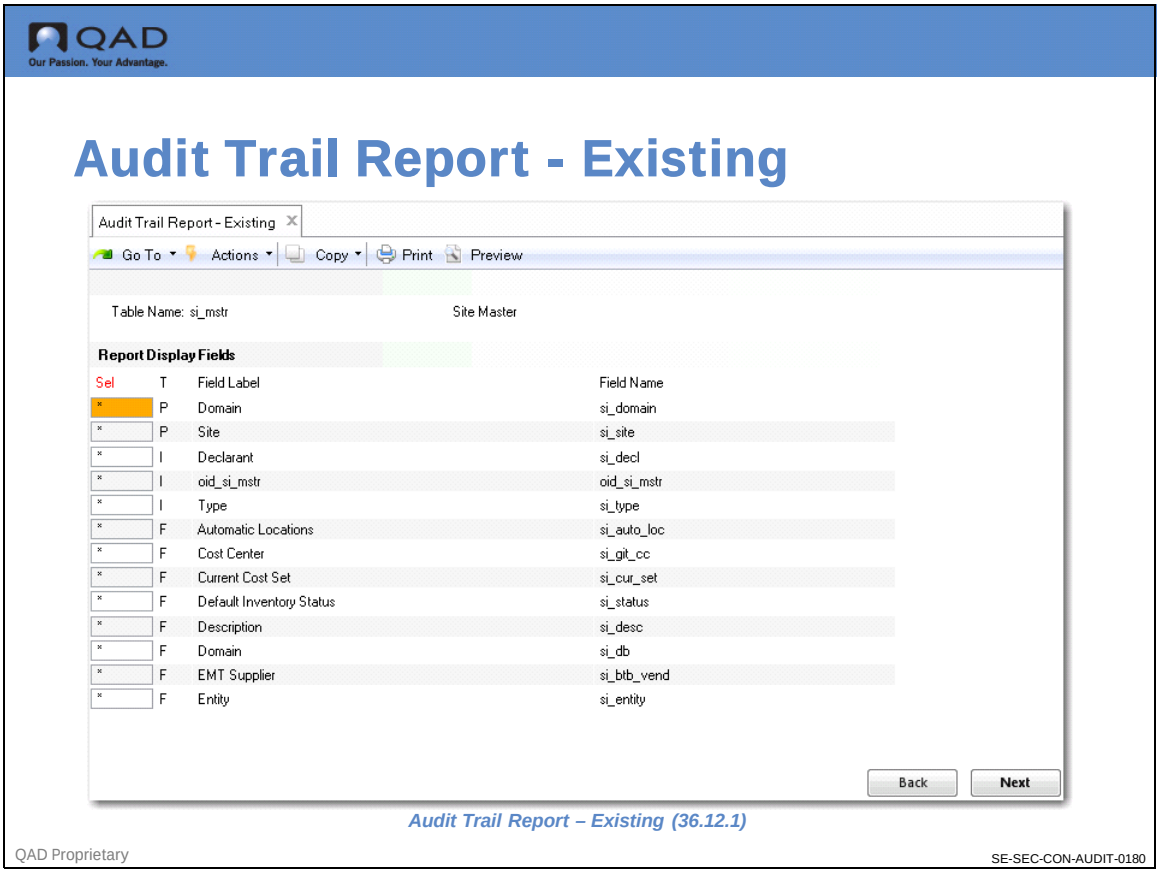
You are not limited by the existing delete event keys. You can select based on any field in the table. Basically you have the identifiers.

In the tier on the left side of the frame, P is for primary index. I represents an indexed field. And F represents Field. The report runs much faster if you select indexed rather than non-indexed fields.

The From and To values allow you to enter a range for that field. Whether you do or do not enter the selection criteria data does not determine if these fields display on the report. It is only affects which records are selected for display.

There is a subsequent frame where you identify which fields to display on the report. This frame allows the user to identify selection criteria for the data report. The user can enter From and To ranges for any field on the table.

Audit Trail Report Existing E-Records Frame 3



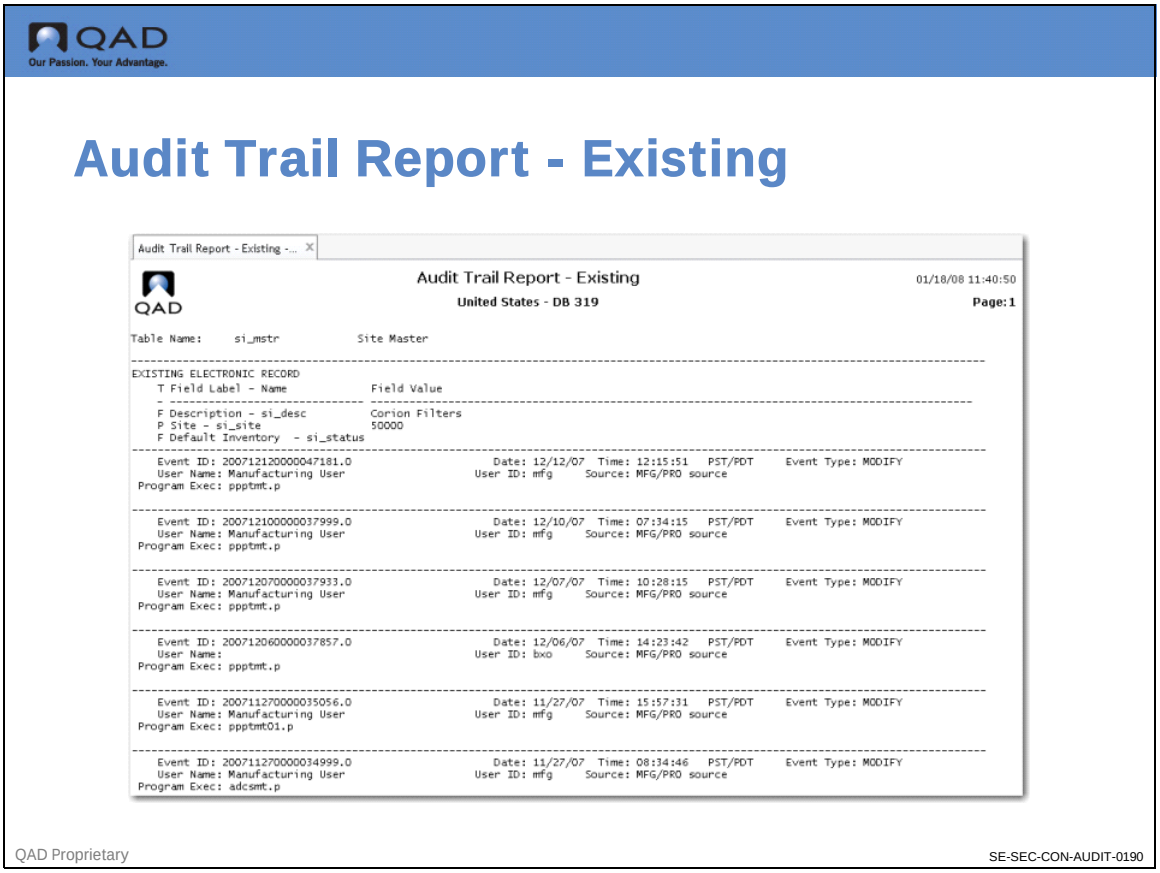
Audit Trail Report - Existing (36.12.1)

This frame allows the you to identify the fields to display on the report, you can select any field on the table.

The default for whether the field is selected or not is determined by the Auto Select All parameter on the first frame. If Auto Select All was set Yes, all fields are shown as selected. You can deselect any fields that you do not wish to display.

The following is an example of the output of the E-Records Existing Report.

Example Report Output



Audit Trail Report - Existing - Output Example

The report shows the details of the existing electronic record. Then it shows the actual audit trail events and the before and after values that were represented by those audit trail events.

Audit Trail Reports Deleted E-Records

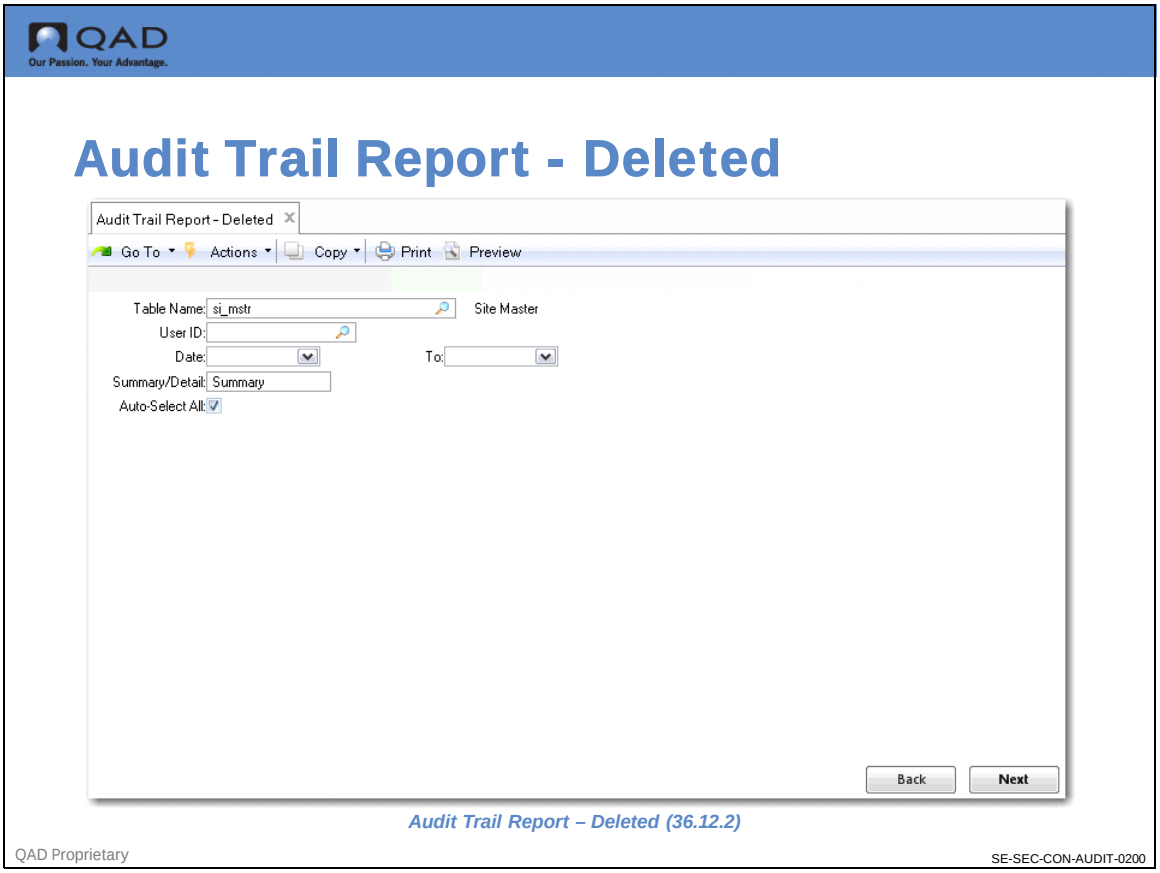
There are differences from the existing report. Filter criteria is by single values, not ranges. This is part of some of the limitations of the indexing possibilities now that you do not have the existing e-record to use as the driver.

The only available filter fields are part of the primary index or those administrator defined delete event keys from audit trail setup through the workbench. An estimated date range for the record deletion event must also be entered as part of the selection criteria.

Another difference is that you need to have an approximate idea of when the record deletion event occurred. This is primary from a performance consideration.

Within these audit databases there is potentially a large amount of Audit Trail data potentially being stored. This is very important for targeting the correct Audit Trail database. Next is the frame for the Audit Trail Report - Deleted (36.12.2).

Audit Trail Report - Deleted (36.12.2)



Audit Trail Report – Deleted (36.12.2)

The fields are similar to the Existing E-Records frame 2 for the report. But in Delete Date, you must enter an estimated date range. This is independent of the date range entered for the Audit Trail transactions on Frame 1.

Audit Trail Report Deleted E-Records Frame 2

The Audit Trail Report - Deleted (36.12.2) E-Records is similar to Existing E-Records Frame 2. In Delete Date the user must enter an estimated date range for the deletion event. This is independent of the date range entered for the audit trail transactions on frame 1. Only single data values can be entered for the filtering criteria.

You still have a date range identified on frame 1 for the Audit Trail transactions.

Example Deleted Records Report

This is very similar to the Audit Trail Report - Existing (36.12.1) and shows the audited table, the Audit Trail events some of the fields for that table.

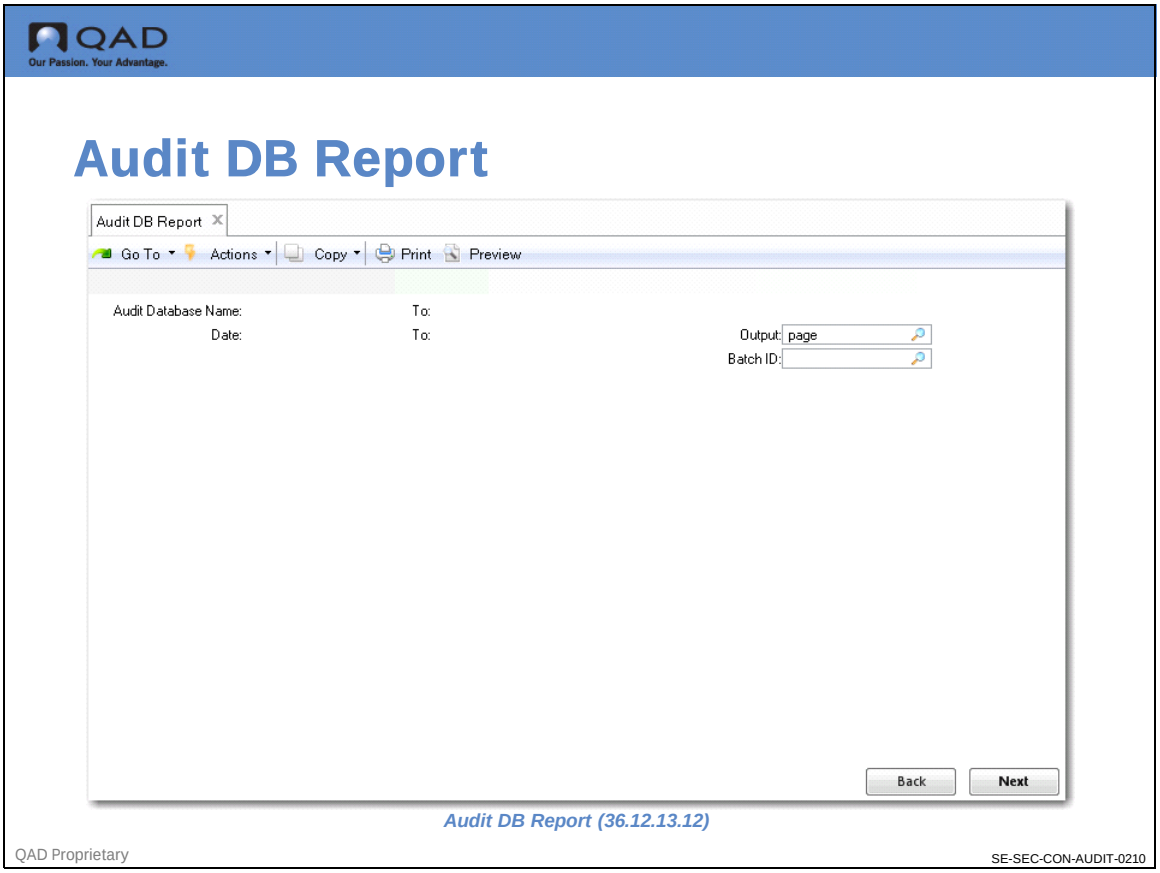
Audit Trail Setup Reports

There are a number of Audit Trail Setup Reports:

- Audit Database Report (36.12.13.12)
- Audit Group Report (36.12.13.2)

- Activated Audit Profile Report (36.12.13.9)

Audit DB Report (36.12.13.12)



Audit DB Report (36.12.13.12)

The Audit DB Report (36.12.13.12.) enables you to report on audited databases in the system.

At any given time, you are going to have a current audit database on the system. But you may also have a number of other databases that are archived and no longer used. However, you may need to have these databases online so the Audit Trail Report can interrogate them to produce a detailed Audit Trail Report.

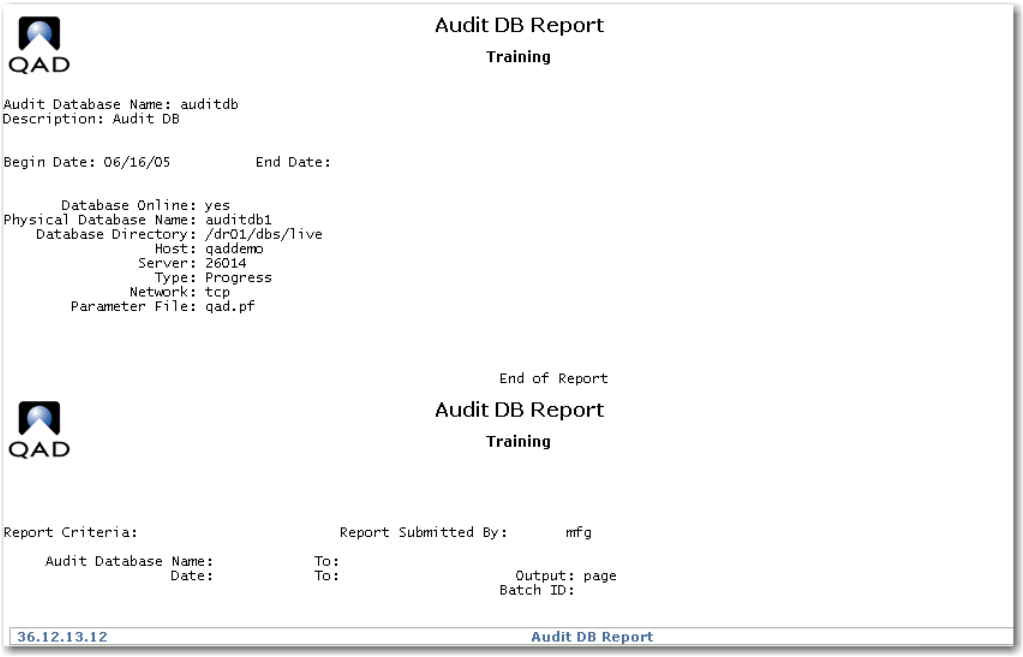
This is why it is preferable to enter date ranges for the Audit Trail data that you wish to report on. This prevents the report from having to search all of the Audit Trail databases for data for a particular record.

These Audit Trail Reports are only going to try to extract information from databases that have that Connect flag set to On.

Audit DB Report (36.12.13.12) -Example Report

QAD
Our Passion. Your Advantage.

Audit DB Report



Audit DB Report

Training

Audit Database Name: auditdb
Description: Audit DB

Begin Date: 06/16/05 End Date:

Database Online: yes
Physical Database Name: auditdb1
Database Directory: /dr01/dbs/live
Host: qaddemo
Server: 26014
Type: Progress
Network: tcp
Parameter File: qad.pf

End of Report

Audit DB Report

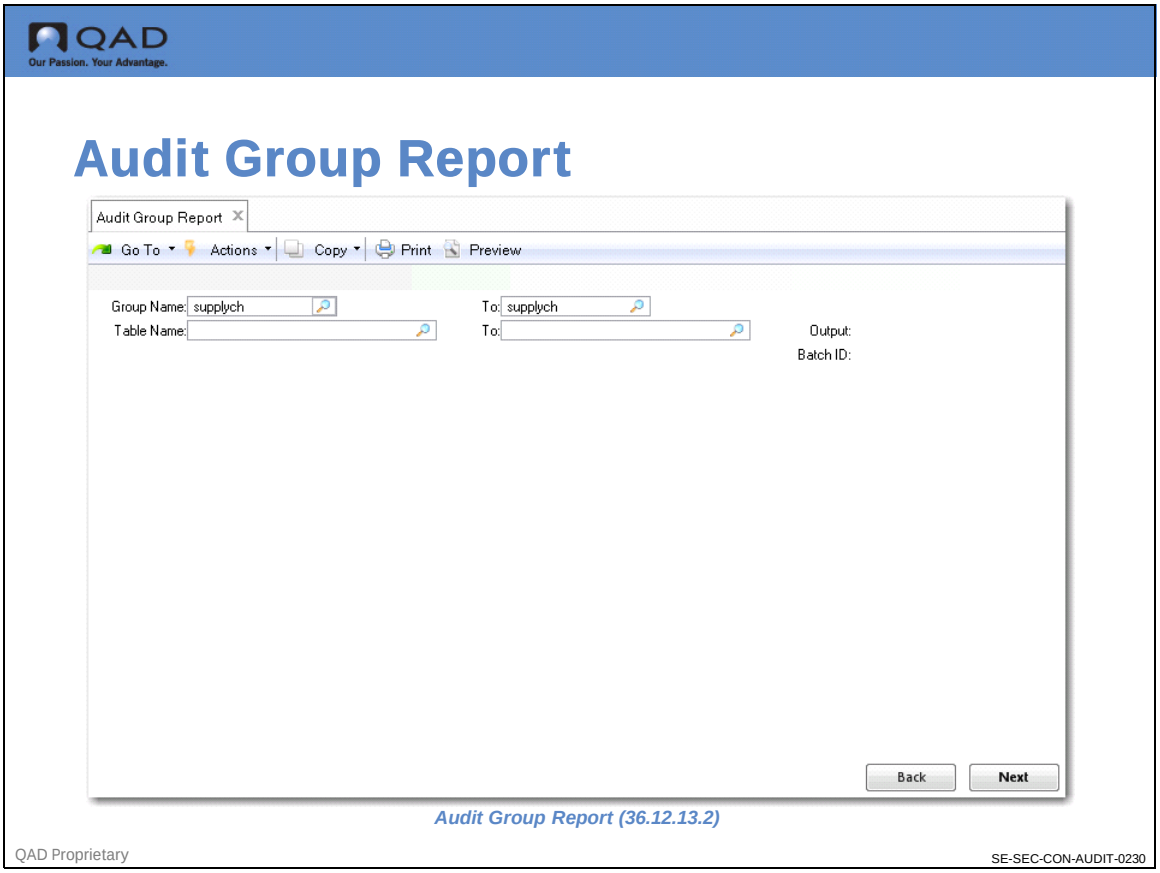
Training

Report Criteria: Report Submitted By: mfg

Audit Database Name: To:
Date: To:
Output: page
Batch ID:

36.12.13.12 Audit DB Report

Audit Group Report (36.12.13.2)



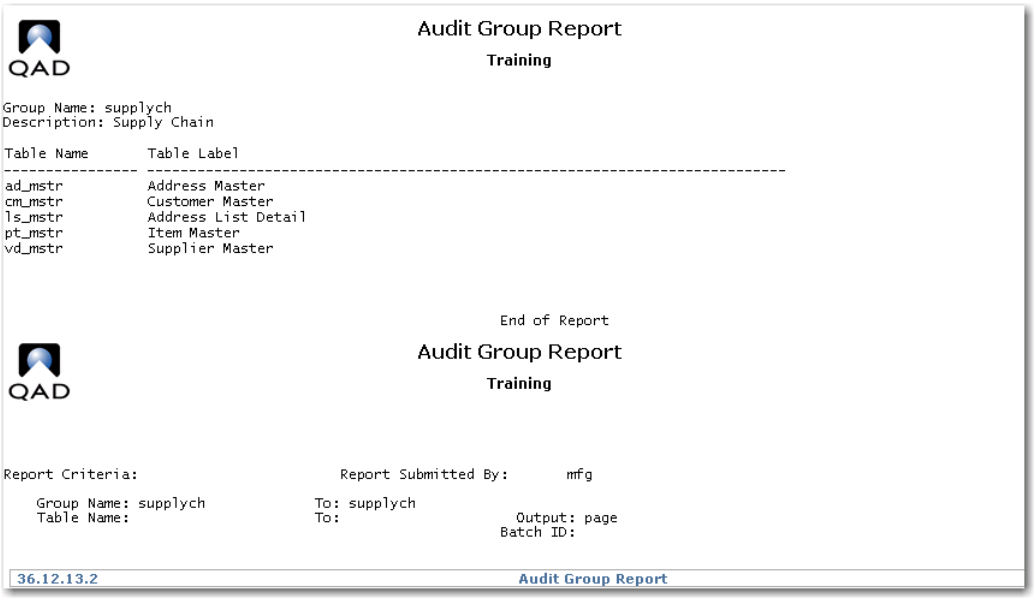
Audit Group Report (36.12.13.2)

In Audit Group Report (36.12.13.2), you can print out the groups that you have available in the table names. You can also specify a table name range. This provides an idea of what tables have been identified for each audit group.

Audit Group Report (36.12.13.2) - Example Report

QAD
Our Passion. Your Advantage.

Audit Group Report



Audit Group Report

Training

Group Name: supplych
Description: Supply Chain

Table Name	Table Label
ad_mstr	Address Master
cm_mstr	Customer Master
ls_mstr	Address List Detail
pt_mstr	Item Master
vd_mstr	Supplier Master

End of Report

Audit Group Report

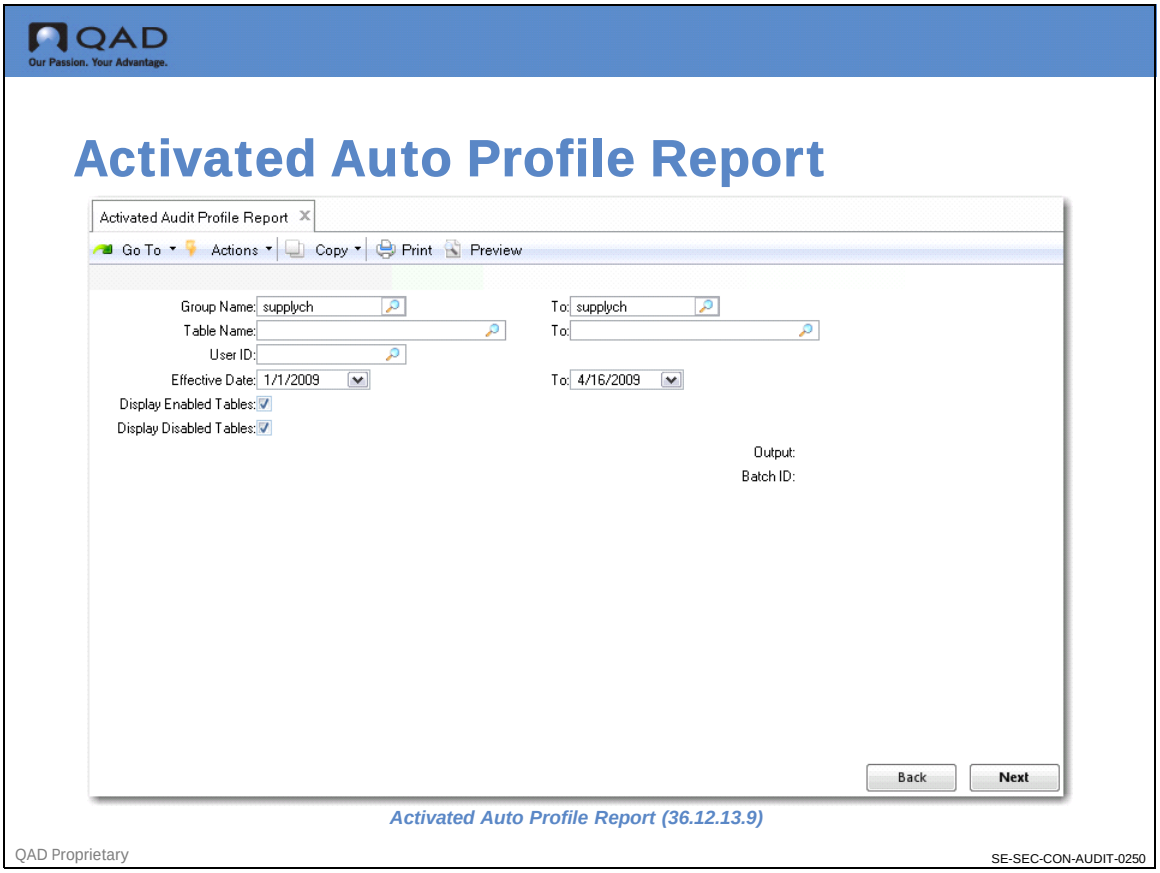
Training

Report Criteria:
Report Submitted By: mfg

Group Name: supplych To: supplych
Table Name: To:
Output: page
Batch ID:

36.12.13.2 Audit Group Report

Activated Audit Profile Report (36.12.13.9)



Activated Auto Profile Report (36.12.13.9)

The Activated Audit Profile Report (36.12.13.9) is a very important because it enables you to identify the active profiles for a particular date range. You can run this report by displaying only those tables that have Audit Trail Enabled or those profiles where tables have been disabled from Audit Trail.

Activated Audit Profile Report (36.12.13.9) - Example Report

QAD
Our Passion. Your Advantage.

Activated Audit Profile Report

QAD

Activated Audit Profile Report

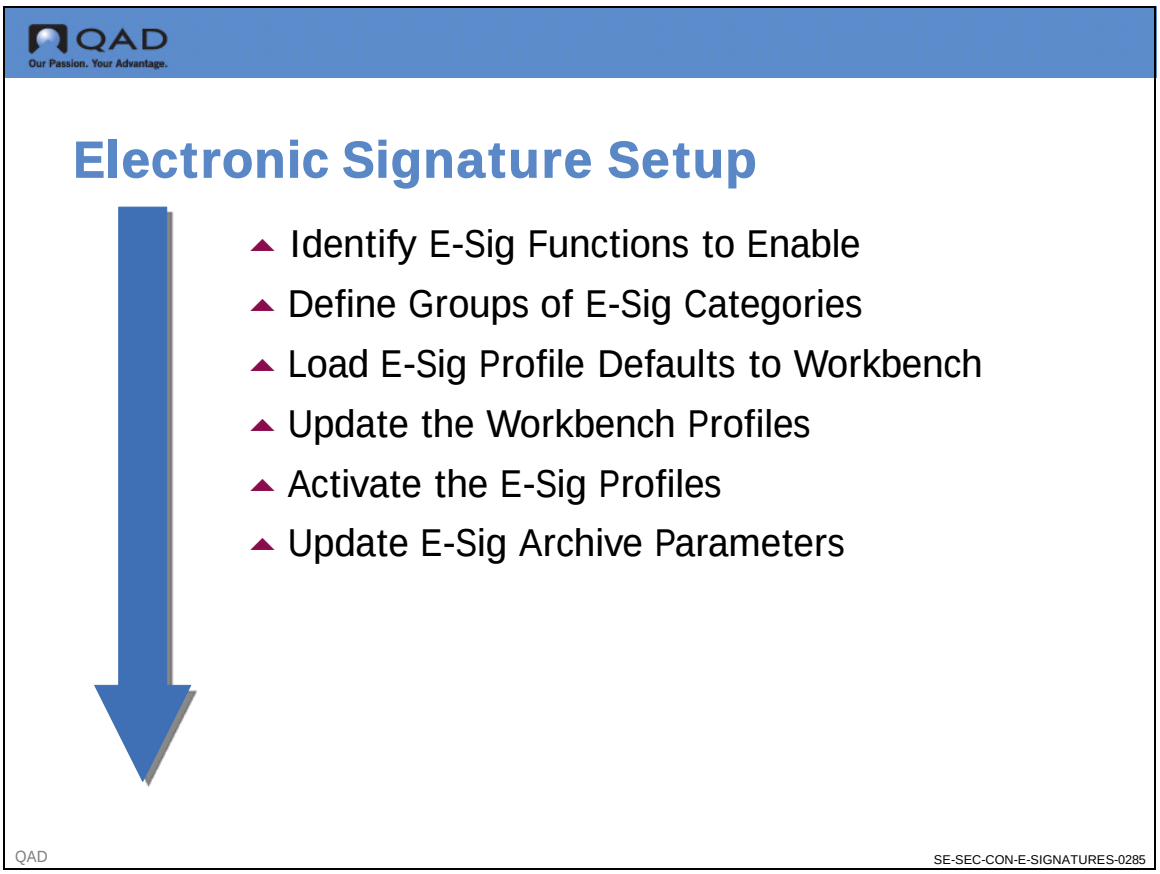
Training

```
Group Name: supplych              Description: Supply Chain

  Table Name: ad_mstr             Table Label: Address Master
    Begin Date: 06/17/05          Audit Trail: yes         User ID: ses

    Field Type     Field Name               Field Label
    ----------     ----------------------   ------------------------------------------------------
    Primary        ad_addr                  Address
    Primary        ad_domain                Domain

Group Name: supplych              Description: Supply Chain

  Table Name: cm_mstr             Table Label: Customer Master
    Begin Date: 06/17/05          Audit Trail: yes         User ID: ses

    Field Type     Field Name               Field Label
    ----------     ----------------------   ------------------------------------------------------
    Primary        cm_addr                  Customer
    Primary        cm_domain                Domain

Group Name: supplych              Description: Supply Chain

  Table Name: ls_mstr             Table Label: Address List Detail
    Begin Date: 06/17/05          Audit Trail: yes         User ID: ses

    Field Type     Field Name               Field Label
    ----------     ----------------------   ------------------------------------------------------
    Primary        ls_addr                  Address
    Primary        ls_domain                Domain
    Primary        ls_type                  List Type
```

Chapter 2

Electronic Signatures

Electronic Signatures Setup



- Electronic signature basics
- Important E-signature concepts in QAD Enterprise Applications
- Execute electronic signature setup
- Execute electronic signatures
- Run electronic signature reports

Electronic Signature Basics

This section discusses a number of areas:

- Why are these features required?
- What are electronic signatures in QAD Enterprise Applications?
- Important QAD Enterprise Applications E-Sig concepts
- Electronic signature setup steps
- Electronic signature function example
- Electronic signature reporting

Why Do We Need Electronic Signatures?

21 CFR Part 11: An FDA regulation, allows for the replacement of handwritten signatures with signatures executed electronically. Instead of having handwritten signatures on documentation, FDA regulations allow for the placement of signatures within the application.

What Are Electronic Signatures?

QAD Enterprise Applications allow for the configuration of sets of data that can be signed in certain menu programs in QAD Enterprise Applications. When configured, these programs prompt for an electronic signature when this data is changed.

Optionally, these programs display the latest signature on record for the data. And finally, the signature is tied to the data via a unique record identifier known an OID value.

Important E-signature Concepts

- E-signature categories
- E-signature profiles
- Signable units
- Signature currency

E-Signature Categories

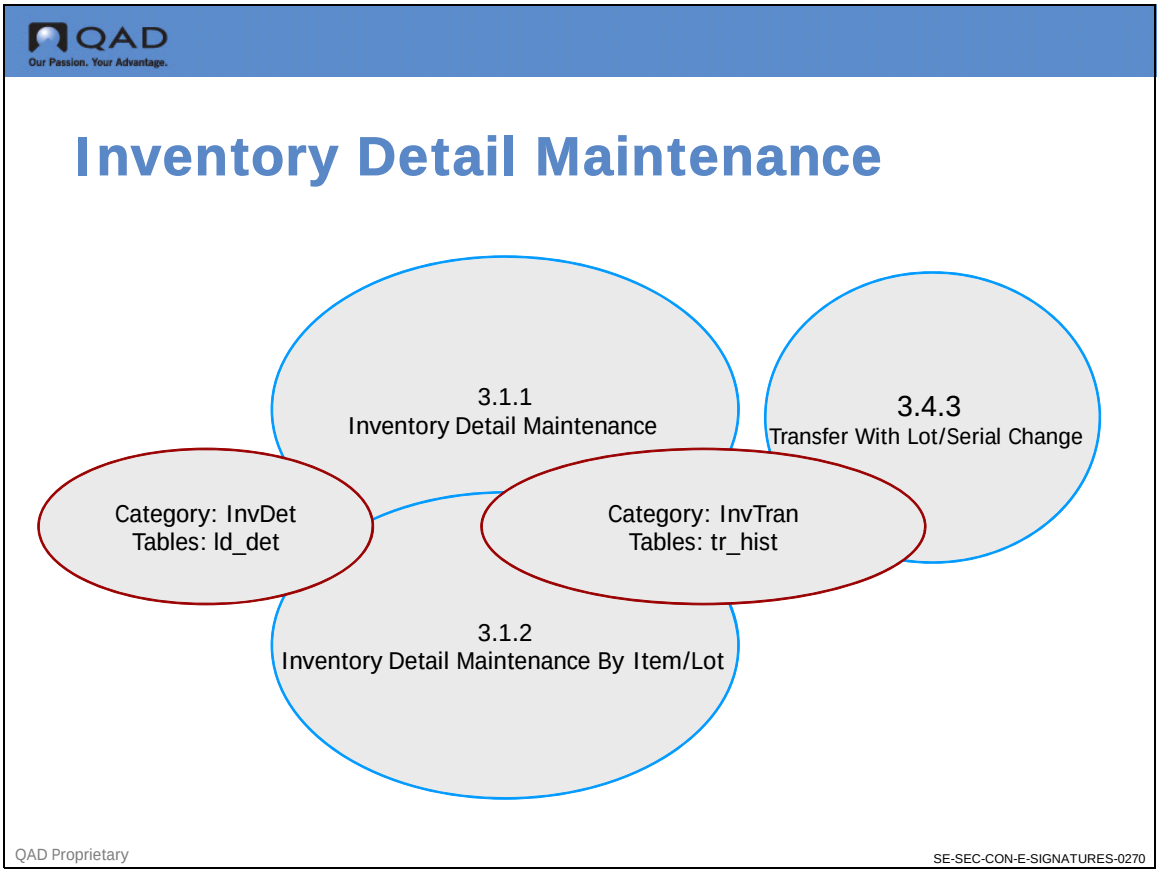
An E-Sig category is the definition of a set of data (tables, fields) that can be signed along with filter fields to determine if a signature is required.

A category profile is a specific configuration of an e-sig category and includes parameters that control E-signature behavior, that is, how the signatures are displayed and how the signatures are prompted for. Category profiles are maintained in a sandbox environment using E-Sig Workbench Profile Maintenance (36.12.14.5).

E-sig categories are associated with menu programs in QAD Enterprise Applications. A single QAD Enterprise Applications menu program may support more than one e-sig category. A single e-sig category may be supported by multiple menu programs in QAD Enterprise Applications.

Menu programs that support multiple categories only require the entry of a single signature.

Inventory Detail Maintenance



Here is a category example for Inventory Detail Maintenance (3.1.1).

Inventory Detail Maintenance (3.1.1) includes two categories: the InvDet category, which includes the ld_det table, and the InvTran category, which includes the tr_hist table. These categories are also shared by Inventory Detail Maintenance by Item/Lot.

InvTran is also shared by Transfer with Lot/Serial Change (3.4.3).

Signable Units

Signable units are instances of e-sig categories. The signable unit is the QAD Enterprise Applications data. These signable units are subject to signature requirements, and are sometimes referred to as category instances.

Active category profiles are used to identify signable units during menu program execution.

The data within a signable unit is considered to be interdependent meaning that any change to a field value within the signable unit should require all of the data to be resigned as a unit.

Example: Inventory Detail Maintenance

This menu program supports two categories, InvTran and InvDet. But why two categories? Why not a single category? One reason is the data involved in these categories are not always updated and created together.

There are other programs where these data elements are updated separately. Also, the signature history for these two sets of data must be maintained independent of each category. Each category instance has a status: Unsigned, Current and Non-Current.

Signature Status

Signable units (QAD Enterprise Applications data), can exist in three states:

- Unsigned: The data has never been signed.
- Current: The data has been signed and the latest signature is current.
- Non-Current: The data has been signed but the latest signature is not current

Current/Non-Current

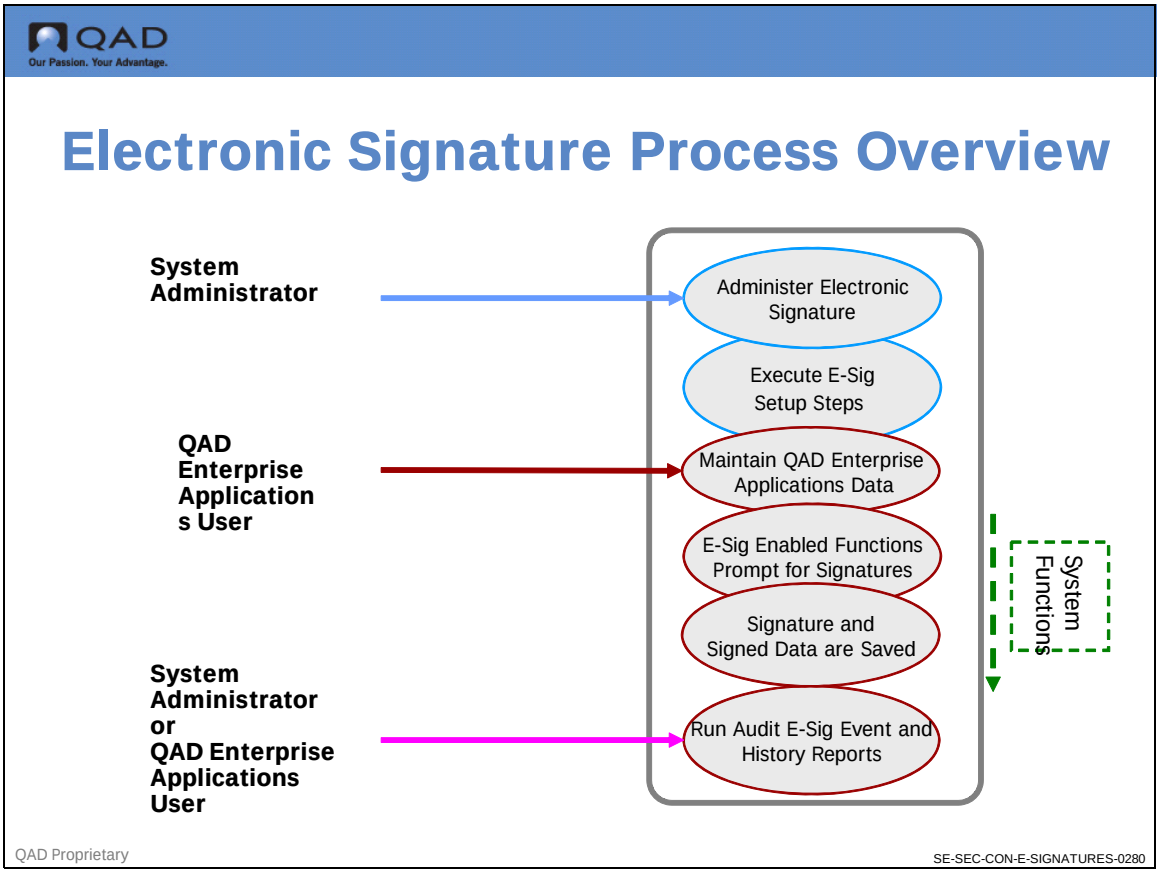
Current signature status means that the signed data matches the current state of the signable unit in the database. That is, the QAD Enterprise Applications data in the database is the same as the data contained in the signature.

Non-current means that the signed data does not match the current state of the signable unit in the database. That is, the database data has changed, but the signable unit has not been re-signed.

Example: Inventory Detail Maintenance

- Inventory Detail data could be updated and signed in Inventory Detail Maintenance (3.1.1).
- This Inventory Detail instance is now signed with a current signature.
- Any subsequent update to the signed fields on the Inventory Detail causes the signature to become Non-Current. The data must be re-signed to regain a current signature.
- If the change is made through non-signature means (e.g. Progress Editor) that data remains Non-Current.

Electronic Signature Process Overview



The administrator sets up the electronic signatures.

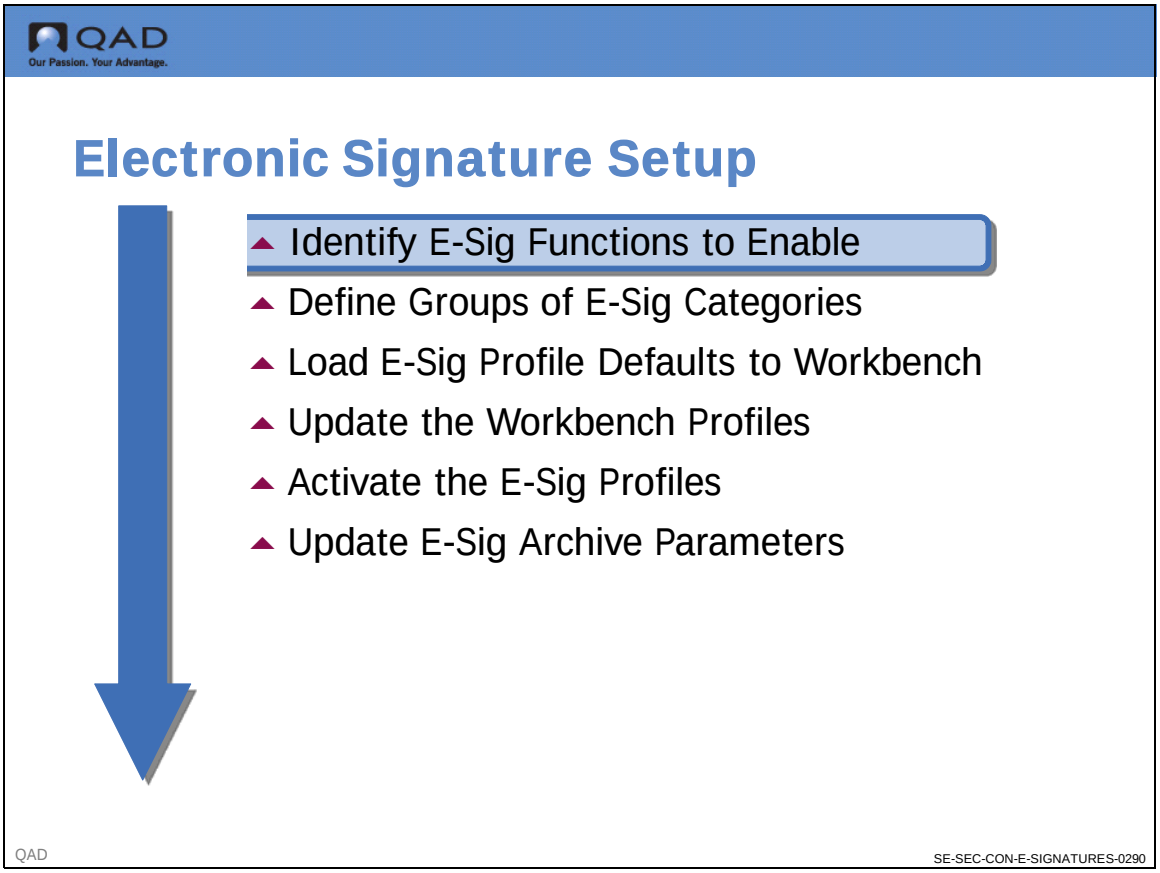
QAD users maintain data. They access e-sig enabled functions that prompt for signatures and they have the signature and signed data saved.

Finally, the system administrator can also run E-Sig Event Report (36.12.4) and E-Sig History Report (36.12.5).

Execute Electronic Signature Setup Steps

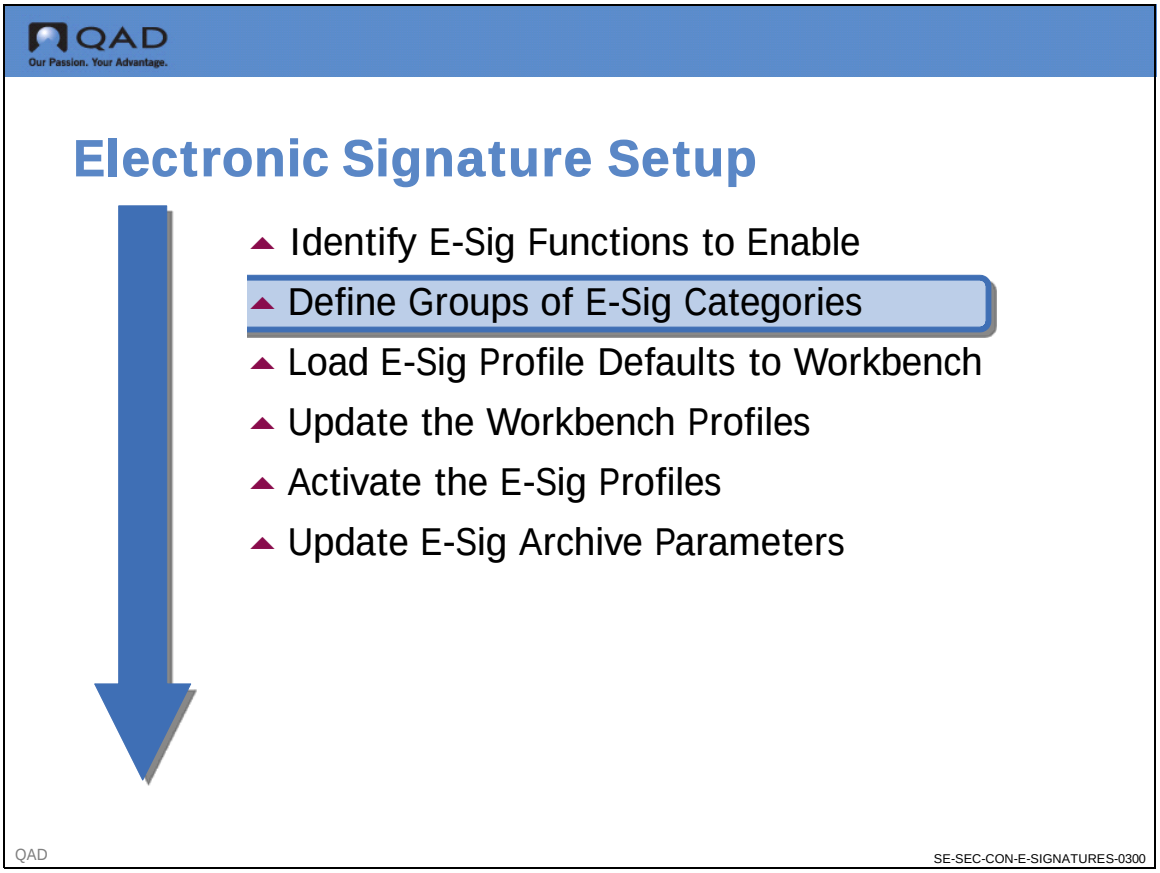
- Identify the QAD Enterprise Applications functional areas to enable for e-signatures
- Identify the e-sig categories available for those functional areas and select the categories to enable
- Define one or more e-sig groups of categories
- Load e-sig category profile defaults to the workbench by e-sig group
- Update the workbench category profiles to identify the signable data and to configure electronic signature behavior
- Activate the category profiles

Identify E-Sig Functions to Enable



Electronic signatures are available in twenty QAD programs, but not all of the programs may be required for a particular business. When enabled, electronic signatures impose additional data entry steps. You must balance the your compliance requirements against the additional data entry burden that electronic signatures impose.

Define Groups of E-Sig Categories

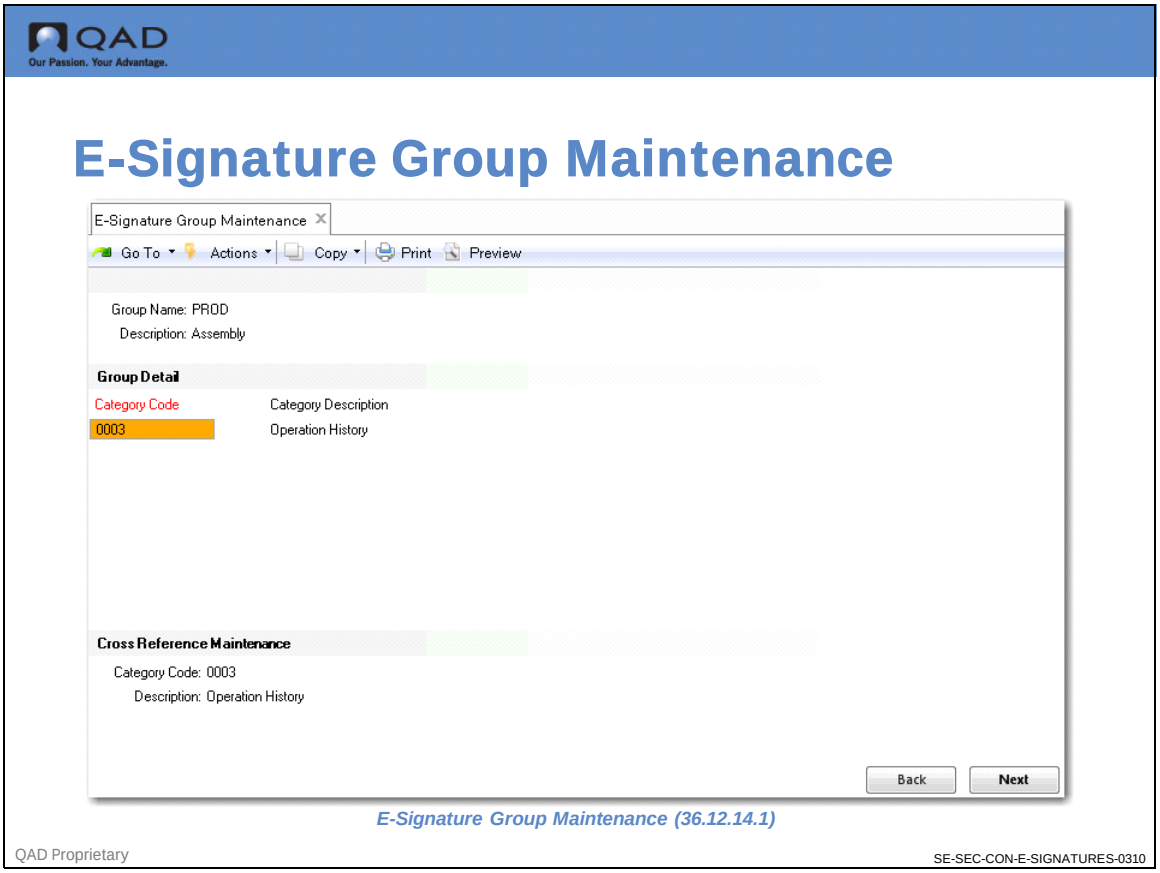


E-sig groups provide a useful way to control and report categories. QAD recommends that you use e-sig categories and e-sig group categories.

E-Signature Group Maintenance

E-signature groups are maintained in E-Signature Group Maintenance (36.12.14.1).

E-Signature Group Maintenance (36.12.14.1)



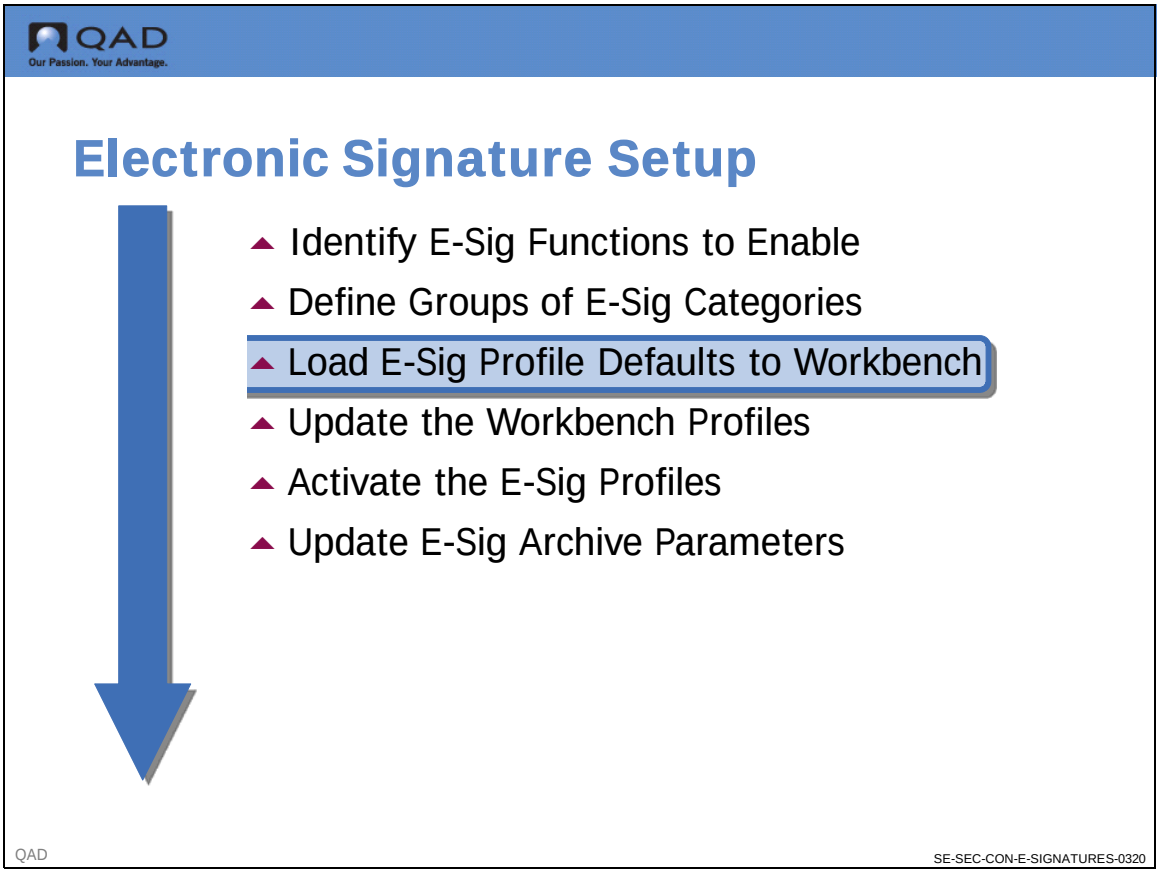
E-Signature Group Maintenance (36.12.14.1)

Group Name. Set to a name that covers all of the categories to activate.

Category Code. Code of the e-sig category to add to this group.

Category Description (display-only). Description of the e-sig category displayed.

Load E-Sig Profile Defaults to Workbench



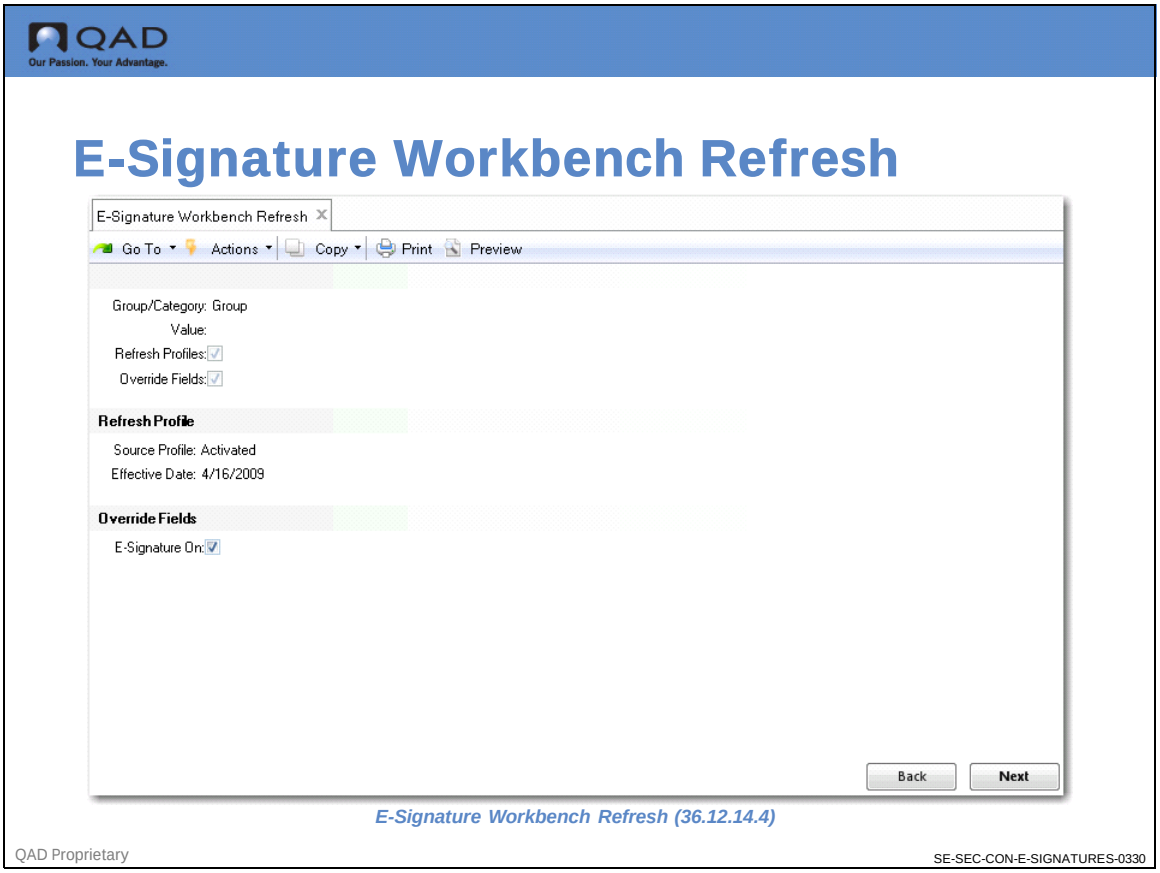
E-Signature Workbench Refresh

Once you have identified your groups of e-sig categories, you can load e-sig profile defaults to the Workbench. This happens through the E-Sig Workbench Refresh (36.12.14.4). That loads category profiles to the workbench and those profiles can be loaded from two separate sources.

The first source is the default category profiles, that are supplied by QAD. These category profiles cover all of the category profiles available for the e-sig enabled functions in QAD Enterprise Applications. The second choice is to load profiles from profiles that have been previously activated.

If you have an activated profile in the system, you can load from there into the workbench to refine your category profiles to reactivate them.

E-Signature Workbench Refresh (36.12.14.4)



E-Signature Workbench Refresh (36.12.14.4)

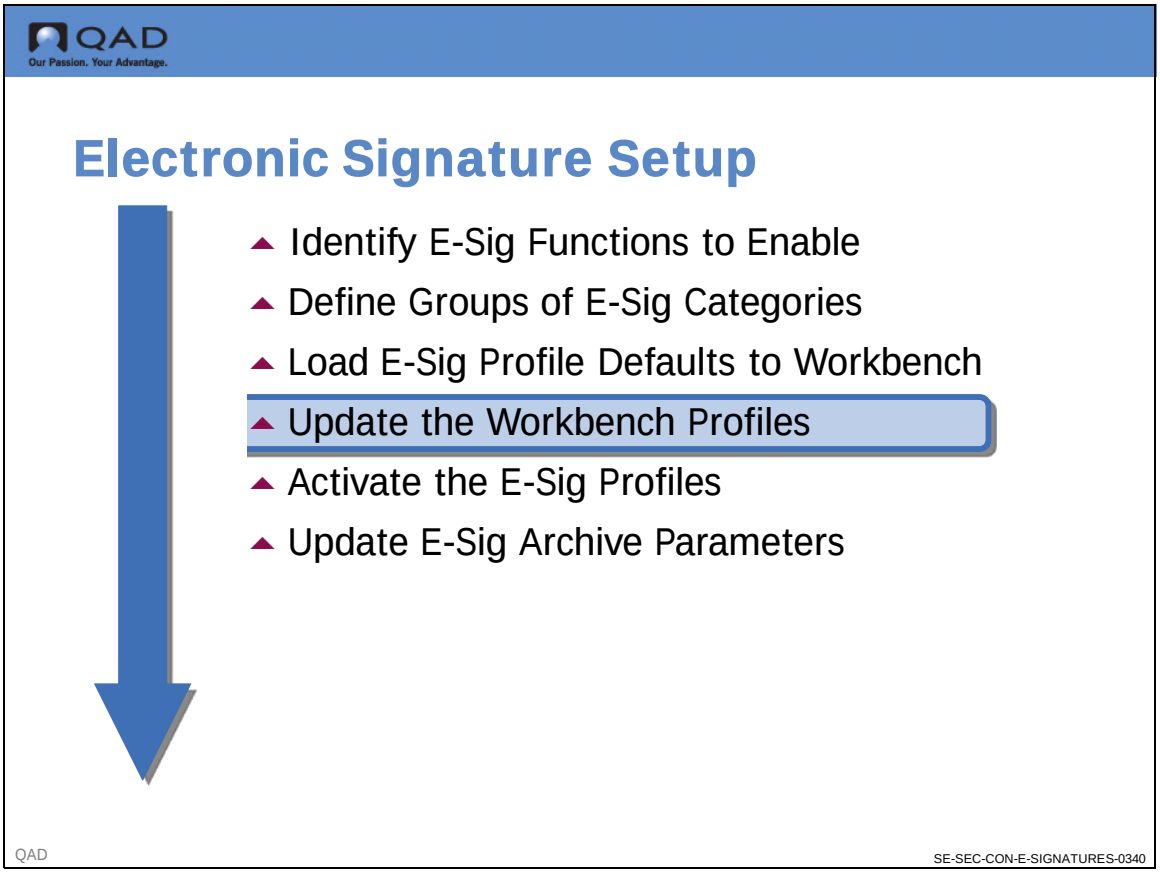
Group/Category. Indicates if the user enters a single category name or an e-sig group name.

Value. The table name or name, depending on group/category entered.

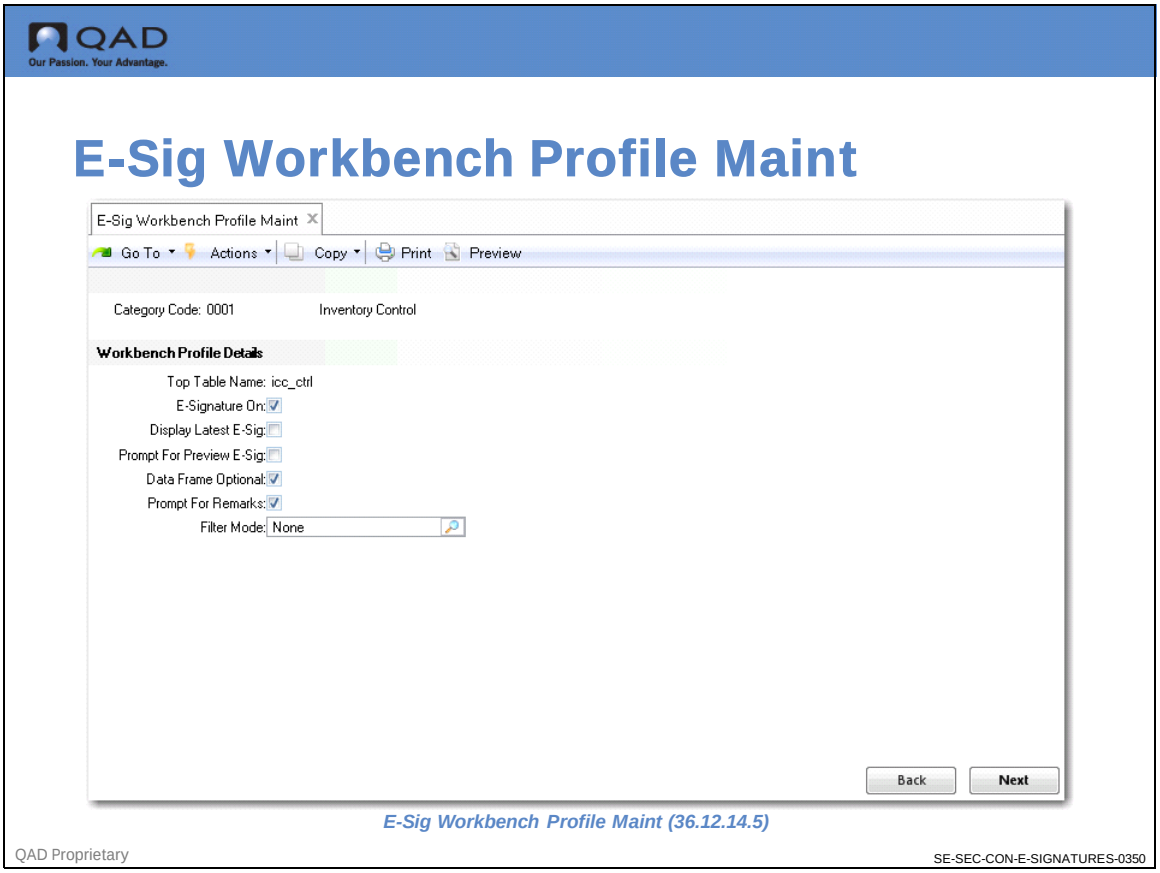
Override Fields. If yes, the user is allowed to set the value for the E-Signature On profile field.

Refresh Profiles. If No, only those fields that can be overridden in existing workbench profiles are updated. If Yes, workbench profiles are created/refreshed and the user identifies the source of the refresh (default or activated profiles).

Update the Workbench Profiles



E-Sig Workbench Profile Maint (36.12.14.5)



E-Sig Workbench Profile Maint (36.12.14.5)

Category Code. E-sig category selected for update.

Top Table Name. Display-only. Provides key values for identifying the signed data. It is required for the e-sig history report.

E-Signature On. Indicates if this category is enabled for e-sig when this profile is activated.

Display Latest E-Sig. Indicates whether menu programs displays the latest e-signature when data from a signable unit is displayed. It is not applicable to all categories.

Prompt for Preview E-Sig. If yes, menu programs prompt for the e-signature after the user has modified the data, but before all transaction data has been created. This prevents unnecessary record-locking and contention problems for programs that create large transactions (for example, labor feedback programs). If no, menu programs prompt for the e-signature at the end of the transaction when all data can be displayed for review. This is not applicable to all categories.

A disadvantage of using Prompt for Preview E-Sig is that the user does not always get to review all of the data before signing. The user-modified data is usually displayed, but not the resulting system generated data. However, when the user is prompted for their signature they can still opt to sign at the end of the transaction by selecting Show Final Data. All of the signed data can still be printed and displayed with the E-Sig Event Report after the signature and the transaction have been completed.

Data Frame Optional. Menu programs prompt for an e-signature using two frames: signature capture (labeled E-Signature) and data (labeled E-Signature Details).

When No, initial focus goes to the data frame where the user can scroll through the data to be signed. The user must enter Next to move to the signature capture frame.

If Yes, initial focus goes to the signature capture frame. The user has the option of moving to the data frame by selecting Scroll Details.

Data Frame Optional is required because an organization may feel that if the default program flow allows the user to not review the signed data, leaving open the possibility that the user can later deny their responsibility for the signed data because they did not know what they signed.

These organizations may feel that this leaves them exposed from a regulatory standpoint. By forcing focus to the data frame, (Date Frame Optional = No) the user has to take action to avoid viewing the data. By the user leaving the frame it is assumed that they have reviewed the data and are taking responsibility for it. This process cannot guarantee that the user will review the data, but reasonable steps have been taken.

Many programs prompt for an e-signature using two frames, the signature capture frame that is labeled E-Signature, and the data frame, that is labeled the E-Signature Details frame.

Prompt for Remarks. If indicated as Yes, this field indicates that many programs that allow the user to enter a freeform remark in the signature capture frame. If set to No, the user is not prompted for this remarks value.

Filter Mode. This specifies the type of filtering the system uses to determine whether the category instance (the QAD Enterprise Applications data) requires electronic signature. The possible values for the Filter Mode are:

- None: Filters are not used. The Filters and Filter criteria frames do not display
- Inclusion: Only data meeting the specified filter criteria require electronic signatures
- Exclusion: All data except those meeting the specified filter criteria require electronic signatures

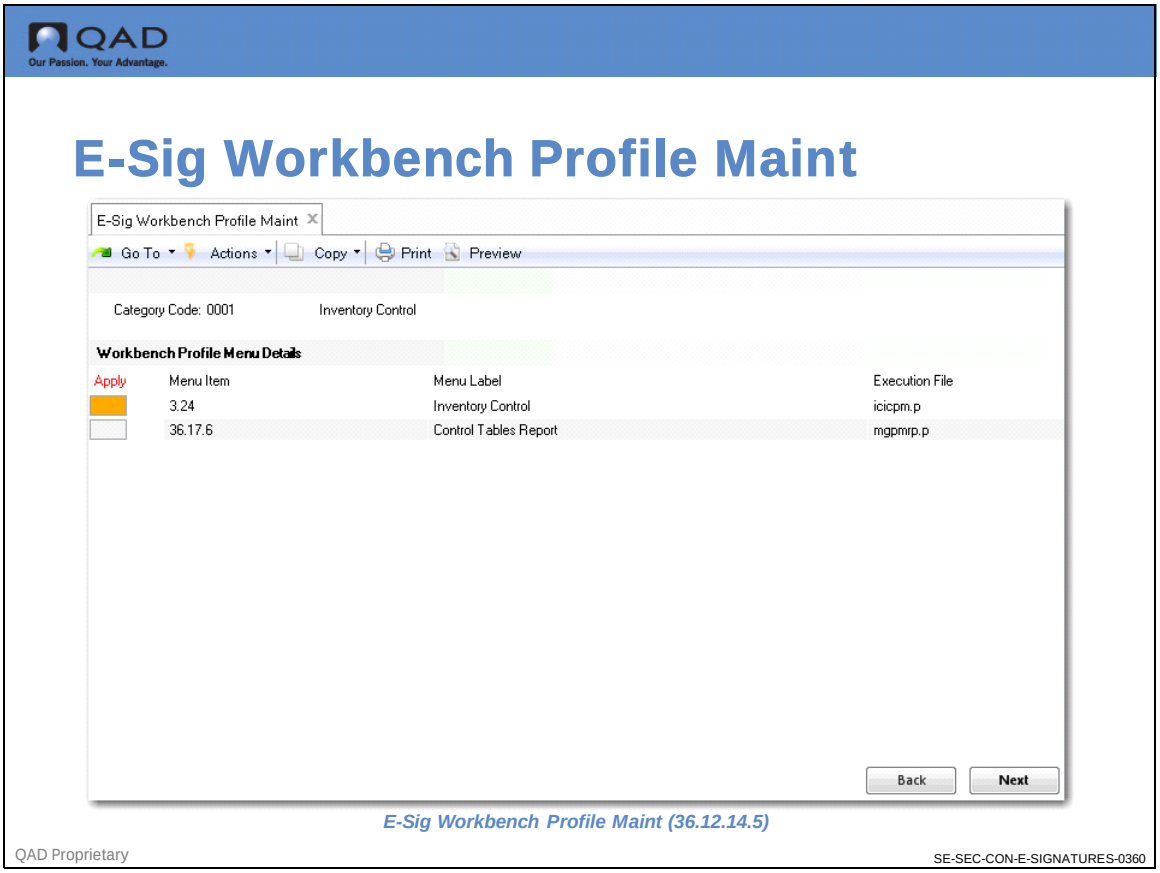
With regard to signable units and the model where signable units are instances of the tables and fields contained in a particular e-sig category, filtering adds a further dimension. Particular instances of the category may be excluded or included from requiring signature based on the values of certain fields within the category instance.

This further refines the idea of what constitutes a signable unit, as characteristics of the data itself can dictate whether the data needs to be signed. This means that only data meeting the specified filter criteria require electronic signatures.

In the electronic signature history report it is possible to display all of the electronic signature events for a particular category. To allow the user to select the signable units to display on the report, a single table is identified from which the user can identify selection criteria.

This table is a parent to the tables present in the category. The top table is also generally one of the tables within the category. However, this is not always the case. It is required by the e-signature history report.

Workbench Profile Menu Details - Frame 2

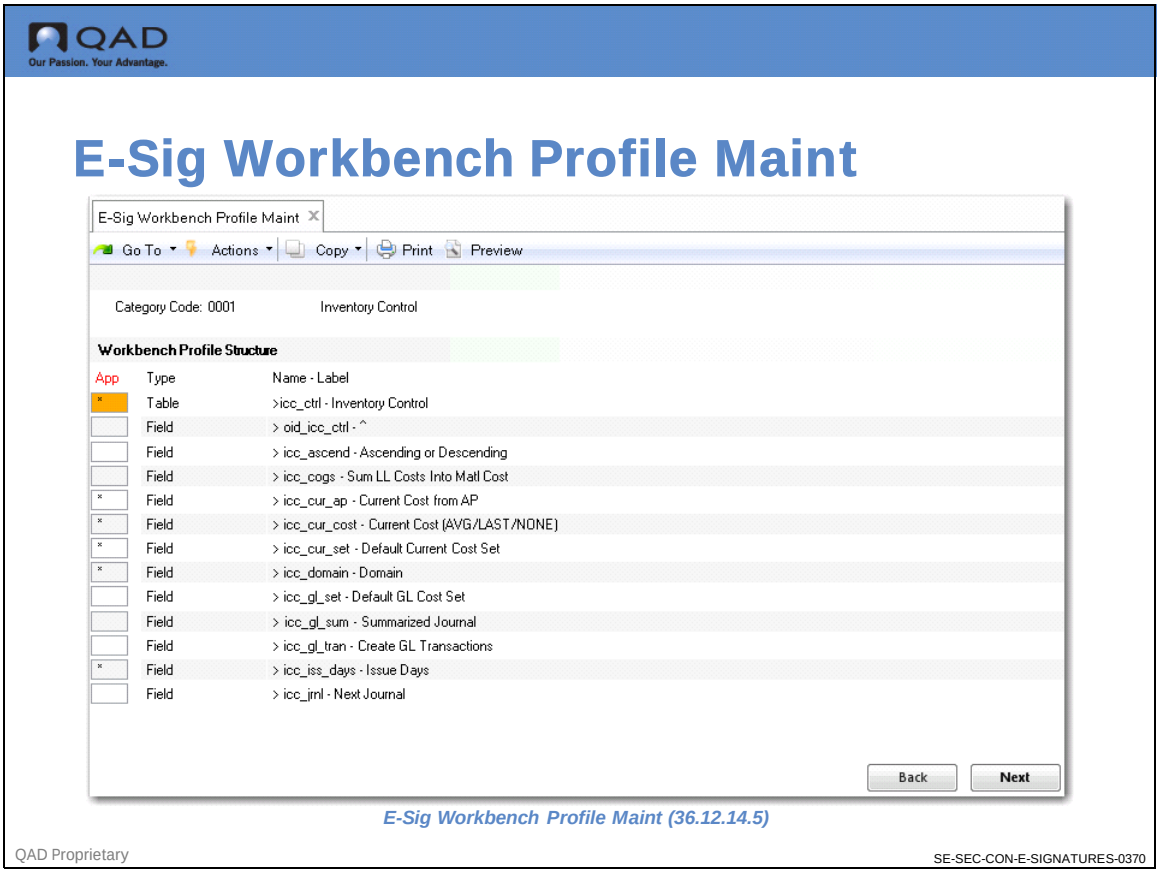


E-Sig Workbench Profile Maint (36.12.14.5)

This frame shows the menu functions available for an e-sig category. In this frame you can indicate whether to apply e-signature controls for this category to this particular menu program.

Many programs cannot be added here. They can only be selected or deselected. The menu programs that are available within a particular category are predefined by QAD.

Workbench Profile Menu Details - Frame 3



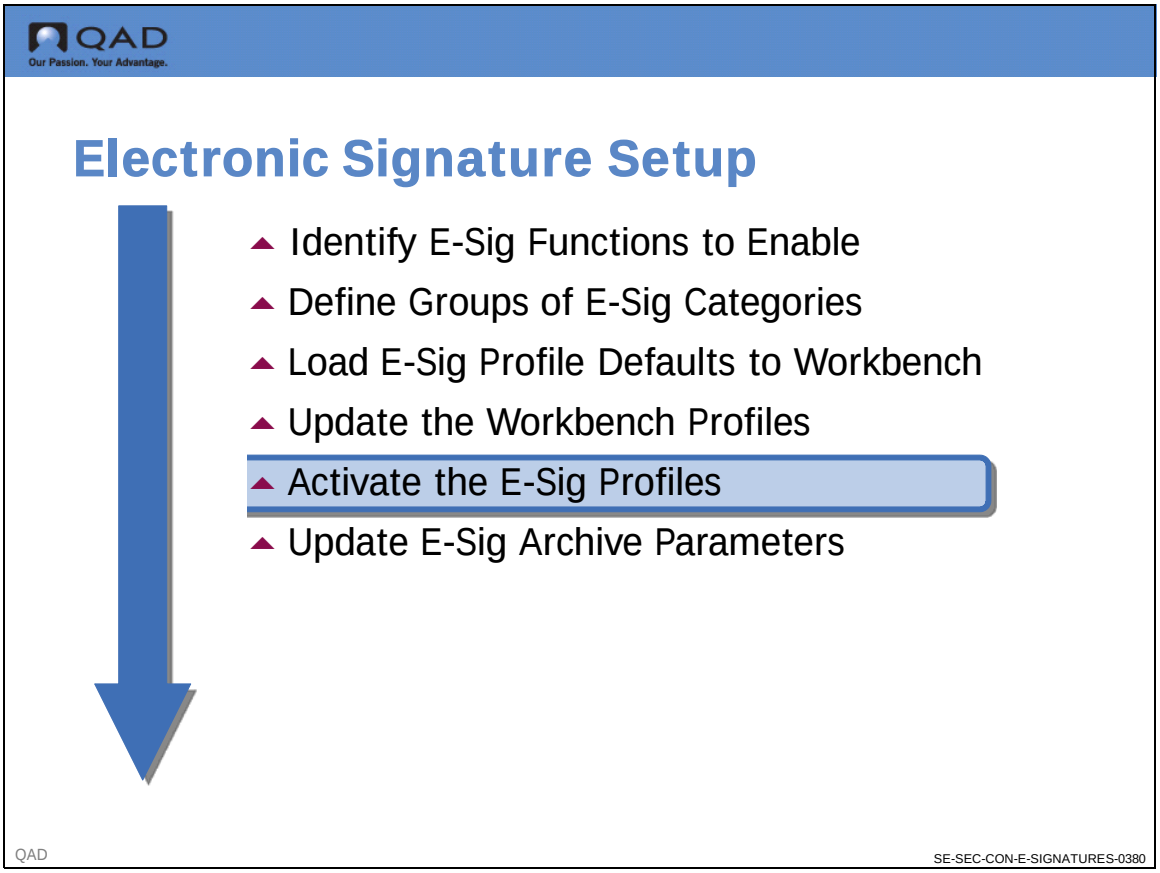
E-Sig Workbench Profile Maint (36.12.14.5)

Workbench Profile Structure

Workbench Profile Structure includes the fields and tables that form part of a category profile.

Workbench profiles refreshed from QAD defaults are created by default with all tables selected and all fields deselected. QAD recommends that selected fields be limited to the minimum required.

Activate the E-Sig Profiles



The final step in electronic signature setup is the activation of the e-sig profiles, which is performed through E-Signature Profile Activation.

E-Signature Profile Activation (36.12.14.8)

E-Signature Profile Activation (36.12.14.8)

E-Signature Profile Activation activates the category profiles that have been maintained and updated through the workbench. You can select to activate by an individual category or group of categories.

Group/Category. Select to activate for a group or a single category.

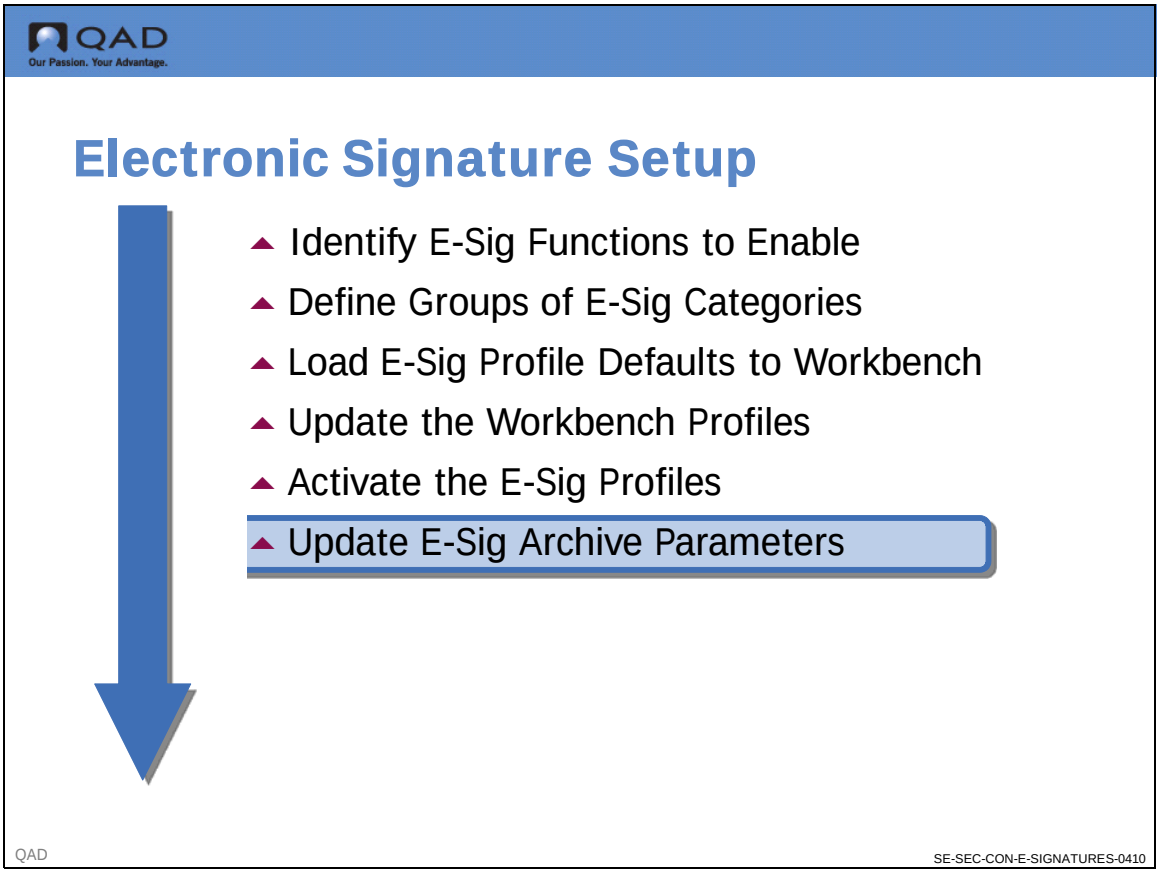
Value. Name of the group or the code for a single category.

Begin Date. Date on which the activated profiles become effective. This must be in the future.

Activate. If not checked, this indicates that the process will run as a report only to indicate the results of the activation of the identified categories without activating them.

In common with other utility functions in QAD Enterprise Applications, you can allow the function to report the effects of running the utility without committing the changes. This ensures an ability to identify the profile that was active on the date that a particular signature was executed.

Update E-Sig Archive Parameters



The final setup step is updating E-Sig Archive Parameters.

Archiving e-sig data is optional and is done done using E-Signature Archive/Delete (36.12.14.22). This process can move e-sig data from the main QAD database to an audit database. It should be used where permissible to free space in the main QAD database.

Before archiving is possible, an audit database must be configured for use with e-sig archive data in Audit Database Maintenance.

Creating an Audit Database

Create an audit database through MFG/UTIL. Instructions for this are found in the QAD Enterprise Applications Installation Guide.

You must then start the audit database servers. Through QAD Enterprise Applications, you can configure the database to store only Audit Trail data, only e-signature archive data, or both.

Within the Audit Database Maintenance you identify the audit database name. This is a unique QAD Enterprise Applications identifier for this database. You can also associate a description with the database.

Audit Database Maintenance Identification Fields

Audit DB Name. A unique QAD Enterprise Applications identifier for this database.

Description. Description of the data base.

Connection Parameters Non-Progress

Database Online is a manual identification whether the database should be currently available. It should be set to No if the database is removed from the system or if the servers are not normally active for that database.

This flag does not indicate if the database can be physically connected to at this time. It is not a check that the system is running against the database to ensure that it is live and available. It is only a manual identification.

This is implemented primarily to avoid attempts by the audit trail reports to open databases that are referenced in Audit DB Maintenance (36.12.13.11), but are no longer available.

Connection Parameters Progress Related

These parameters are the same as those identified in Database Connection Maintenance (36.6.1).

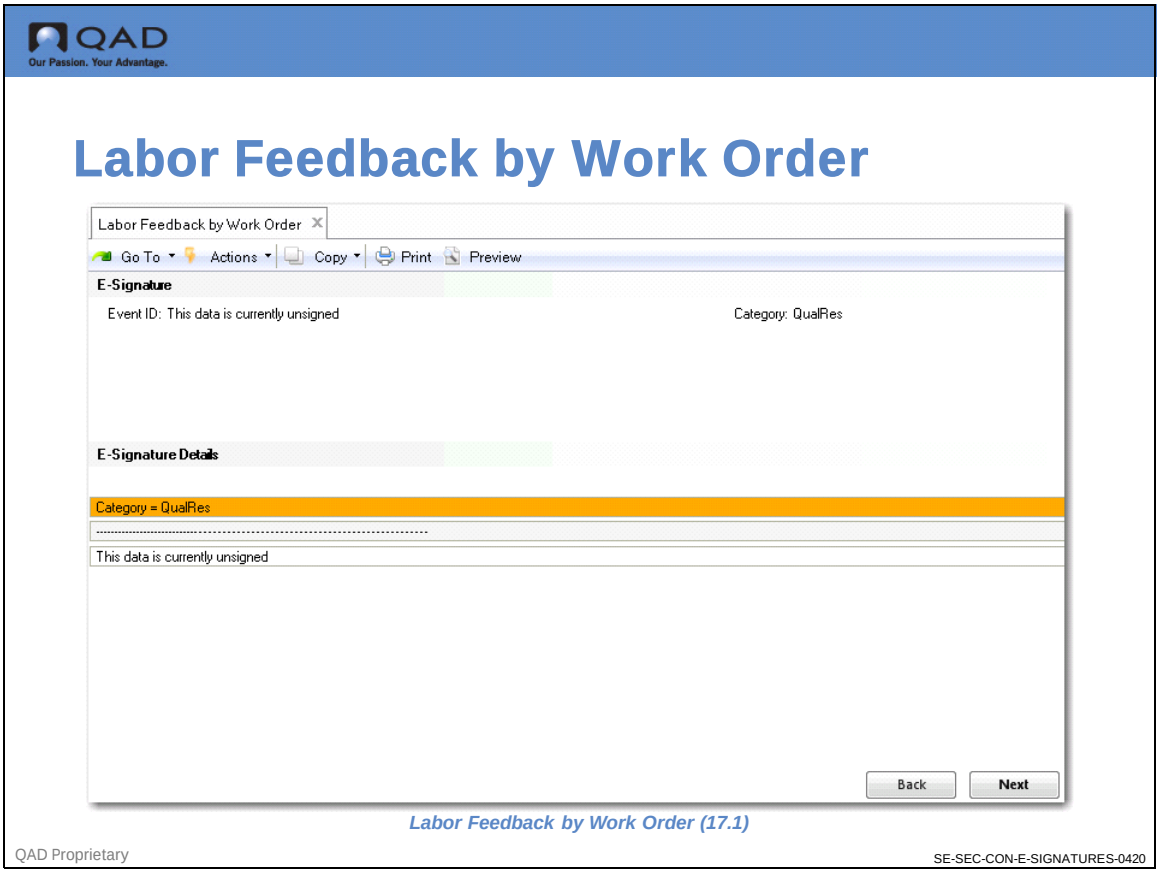
The rest of the parameters are all Progress-related. They only relate to information such as the sort of a connection to establish with the database and what the host and the server names are. Refer to Progress documentation for further details of these parameters.

The next step in the Audit Trail setup process is identifying the QADDB tables to audit trail.

Database Type

E-signature indicates if archived e-sig data is to be stored in this database. Begin Date is the date this database comes online and become the current e-sig archive database. It is important to note that no two e-sig archive databases can have the same Begin Date. End Date is automatically filled by the E-Signature Archive/Delete process when the next audit DB is used.

Example: Execute Electronic Signatures



Labor Feedback by Work Order (17.1)

Here is an example where electronic signatures have been implemented in Labor Feedback by Work Order (17.1).

First, the Labor Feedback by Work Order record is selected. The Display Latest E-Signature frame. This frame displays only if Display Latest E-Signature is enabled for this particular category.

Latest Signature Display

The frame indicates that the event is unsigned, this means that the data has just been created or it has not been updated through Labor Feedback by Work Order after e-signatures was enabled.

If you update any of the signed fields on Labor Feedback by Work Order you are prompted for the e-signature.

Next the data is updated in Labor Feedback by Work Order.

Prompt For Preview E-Sig Frame

If the prompt for preview e-sig is configured for the active category profile, in this case wr_route, this frame appears next. It must be noted that since this is a program where the changed data is committed as a transaction at the end, the data being signed cannot be seen in the E-Signature Details frame. If the user decides not to view the final data, they can complete entry of the signature details and finish signing on this frame.

If there is a need to review the data, which may be related to the organization’s standard operating procedures, selecting the Show Final Data option allows the user to sign at the end of the transaction where the final data is available for review.

This frame only displays when Prompt for Preview E-Sig is selected for the currently active category profile.

If required, the user can select to Show Final Data to complete the signing at the end of the transaction for this category profile, remembering that this is the Prompt for Preview E-Sig frame. The focus is initially on the bottom frame if Data Frame Optional is set to No for that active category profile.

In the Prompt for Preview E-Sig frame, the signed data is not available until the transaction is complete. That is indicated in the bottom frame by the text, Final Data is Not Available.E-Sig Final Details Frame

If the user selected Show final Details from the preview frame or if Prompt For Preview E-Sig was not selected for this category profile, the Final Details Frame displays. As with the preview frame, whether the initial focus is on the e-signature frame or the e-signature details frame is directed by the Data Frame Optional configuration for the active category profile.

In this frame the user enters the signature details. If the user selects the Scroll Details option, the focus shifts to the bottom frame to allow the user to browse through the data to be signed.

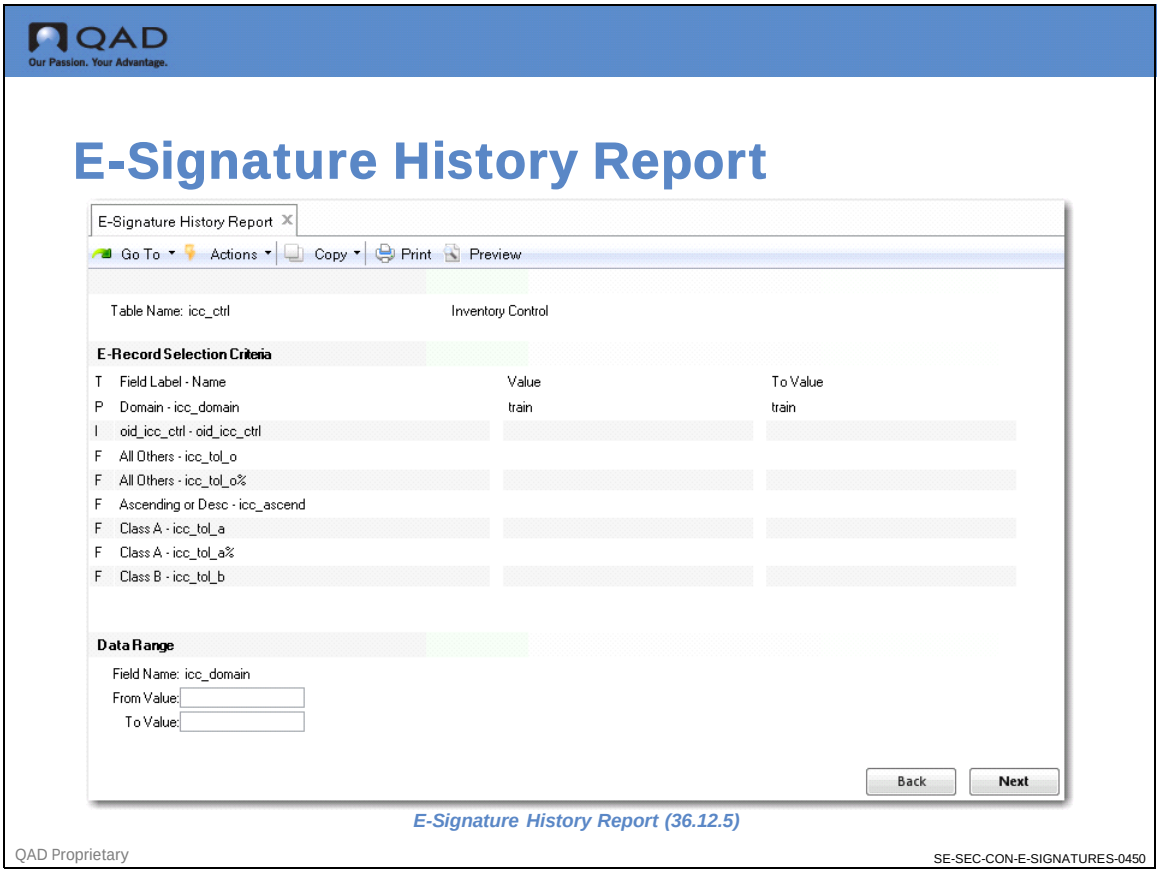
The data to sign is now available in the bottom frame (it was not available in the Prompt for Preview E-Sig frame).

Once you have signed the data, you must check the latest e-signature. Return to the Inventory Detail Maintenance function. If Show Latest E-Signature is specified for this category after you have moved through the top fields in the frame, the latest e-signature is displayed.

When you re-enter the program, select the record that you previously updated and signed. The top of the frame displays the e-signature details (the Event ID) if the signature is current, the reason code for that signature, the category, and the e-signature execution date.

In the bottom frame is the signed data for that particular signature category. The user may scroll through the data because all of the fields may not appear on the screen.

E-Signature History Report (36.12.5)



E-Signature History Report (36.12.5)

The first of the electronic signature reports that you need to review is the Electronic Signature History report. This report displays the individual signature events without regard to the subject data and can display summary or detail information.

This is the initial frame for the Electronic Signature History report. You can select the Electronic Signature History Report to operate for a particular category. On this screen, once you have selected the Category Code, the Table Name appears.

This is the Top Table Name identified for this category. It identifies the data the report navigates through to get to the signature events.

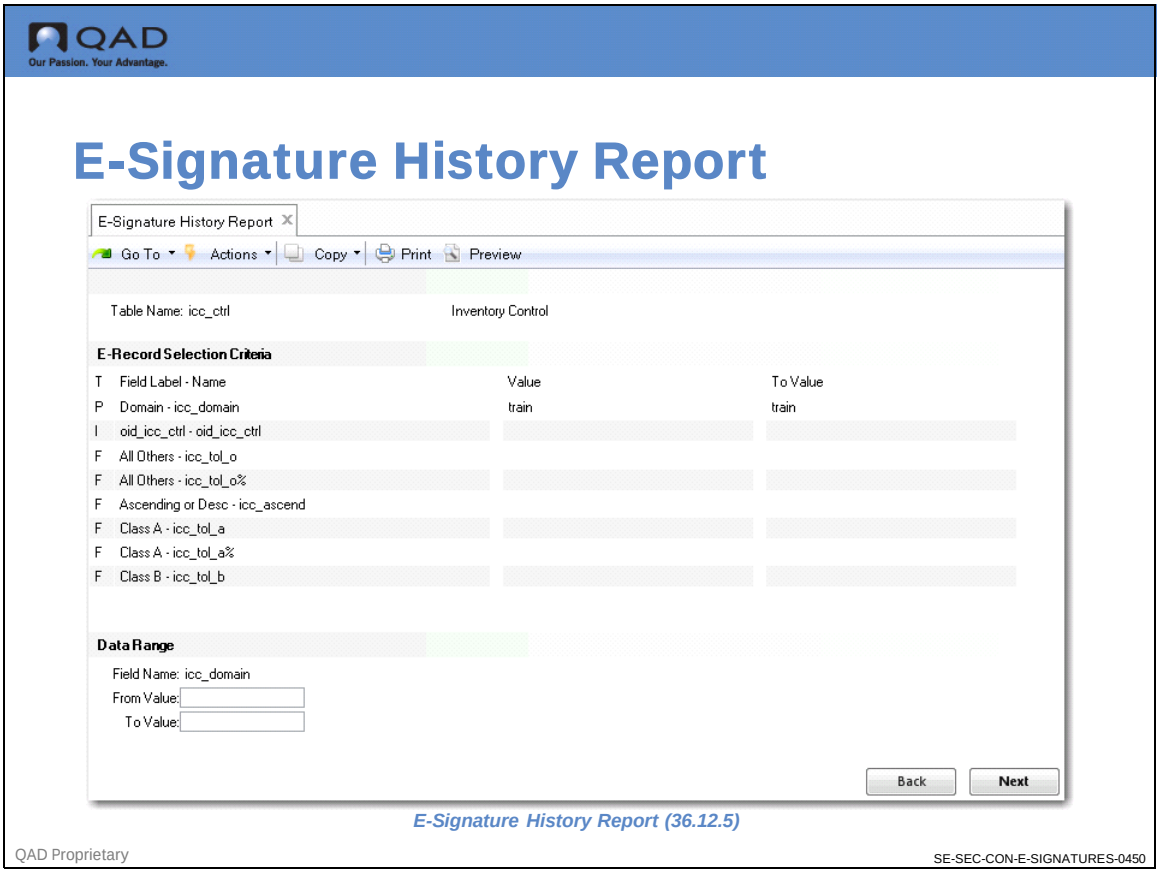
For the report you can also enter a User ID range, an Electronic Signature Date range, and a maximum number of electronic signature events (Max Events). You can limit the number of events to display for each signable unit.

Entering a 1 shows only the latest e-signature for each signable unit selected. You can select the report to display only the current e-signature. This limits the selection to only those signable units with a current electronic signature.

You can also elect to display where the Table Data is unsigned. This displays where the signable unit has never been signed. This option can add time to report generation. Auto-Select All defaults the Sel value on the Report Display field screen to be selected.

In an upcoming screen, you can identify those fields that you wish to display for the signed data on the report, and this value enables you to default the selection to all of those fields.

E-Record Selection Criteria

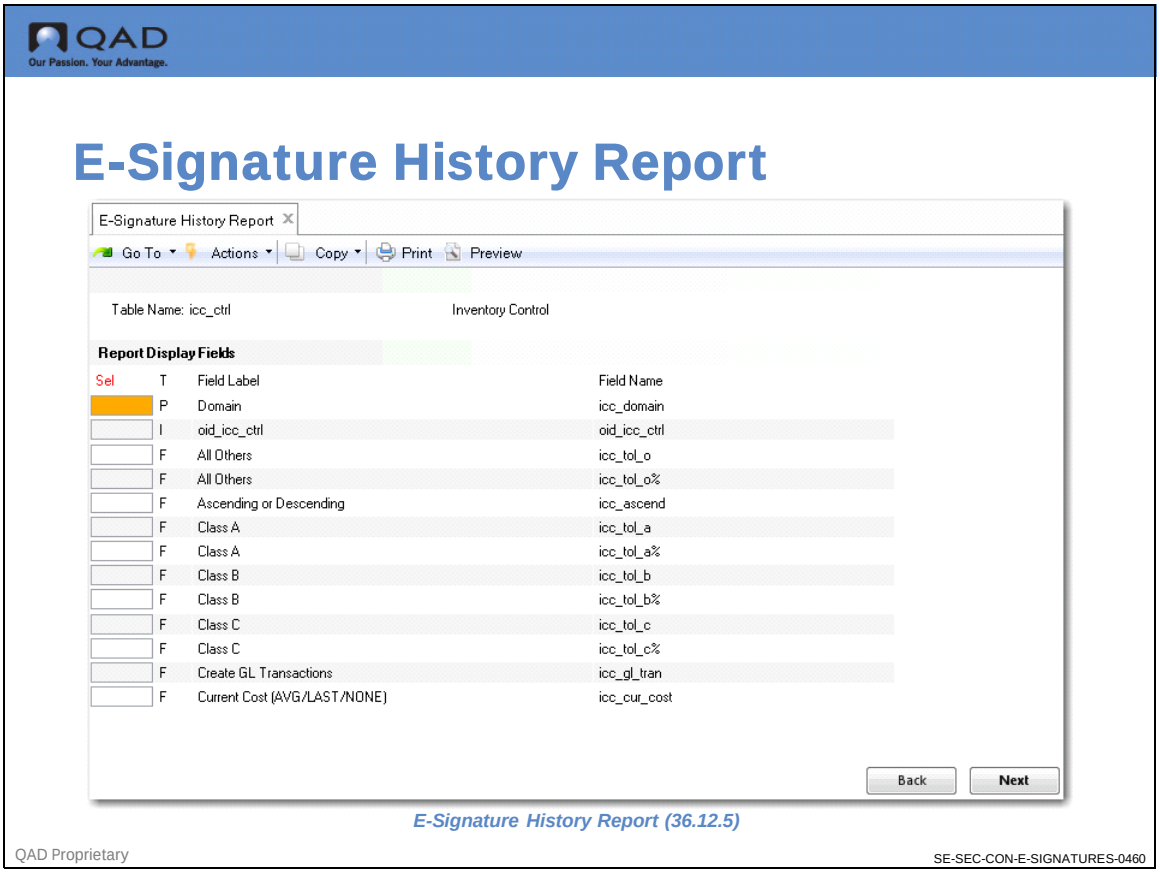


E-Signature History Report (36.12.5)

This allows for the filtering of data by the values in fields in the top table. The data ranges entered here relate to the top table that has been identified. A T indicates the field type. This can be one of Primary Index, Index or Field. This can be useful in entering your selection criteria to ensure that the report operates in the fastest possible manner.

Selecting fields that are a part of primary indexes or regular indexes produces faster report execution. Field label is the name of the field. The Value and Value To are the value range entered for the selected fields.

E-Signature History Report (36.12.5)



E-Signature History Report (36.12.5)

SE-SEC-CON-E-SIGNATURES-0460

Report display Fields

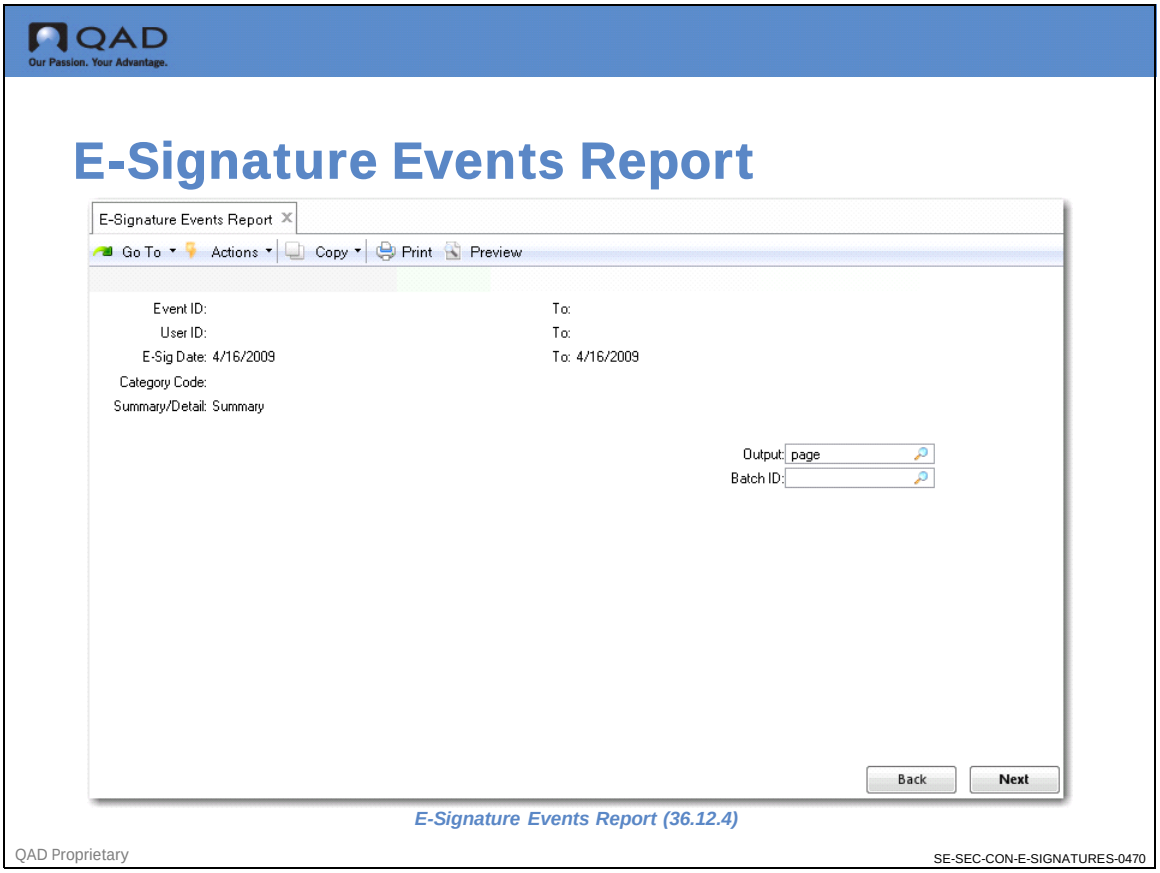
You can default the Sel value on this frame to select all of these fields or to select none of them. That is useful if you only wish to display one or two fields.

Next you set the Sel value on the previous frame to No and then individually select each field.

If, on the other hand, you wish to select most or all of the fields, you would enter Yes for the Sel value on the previous frame and and deselect those fields you did not wish to display.

The fields selected here do not affect the fields displayed in the actual signature data. All of the signed fields are displayed within the signature data. This only deals with the display of the data from the top table.

E-Signature Events Report (36.12.4)



E-Signature Events Report (36.12.4)

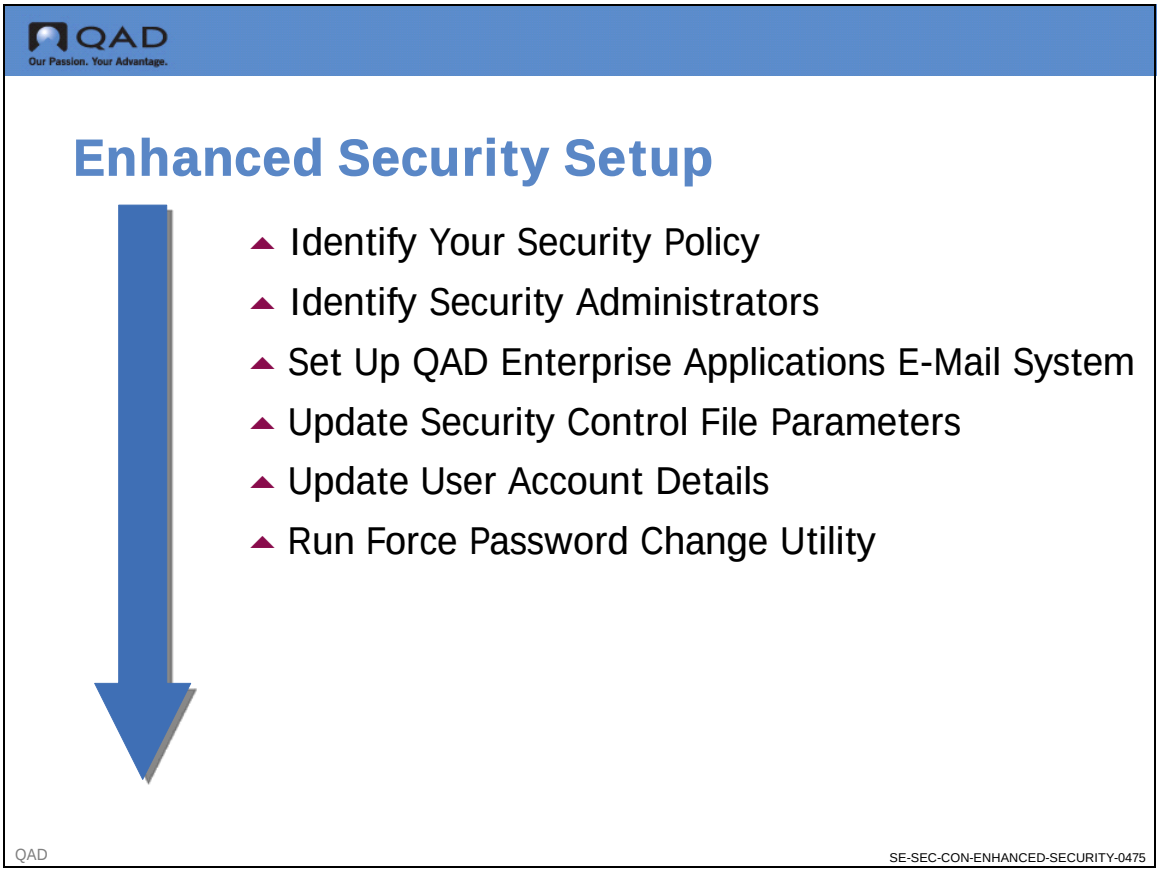
This displays the individual signature events without regard to the actual subject data. It goes directly to the signature events in the database. This report can display summary or detail information.

You can enter an Event ID range, User ID range, and an E-Signature Date range. You can identify whether to print for a specific category code or for all category codes by leaving that value blank. You can then opt to also display summary or detail information.

Chapter 3

Enhanced Security

Enhanced Security Setup



This chapter covers:

- System controls and security basics
- New security reports

System Controls and Security Basics

- Why do we need enhanced security in QAD Enterprise Applications?
- What new features have been added to the application?
- What are the security setup steps?
- What changes to the administration of functions?

Why Enhanced Security?

Much of QAD's attention to security is directed at the requirements of 21 CFR Part 11, a regulation related to computerized systems that mandates that users be held accountable for their actions.

Enhanced Security is designed to prevent users from denying responsibility for their online activities by claiming they were not logged on to the system and someone else was using their logon account.

What are System Controls and Security?

To support this requirement, QAD has made changes in three basic areas. First QAD created advanced password characteristics. They allow for a much more rigorous approach to password structure with supporting additional controls for password aging and reuse.

The second area involves enhanced user account administration. QAD created a capability to separate account administration from password allocation. Therefore, the person administering the account is not directly responsible for allocating initial passwords. In addition, the product ensures the validation of user group names and allows for the deactivation of user accounts.

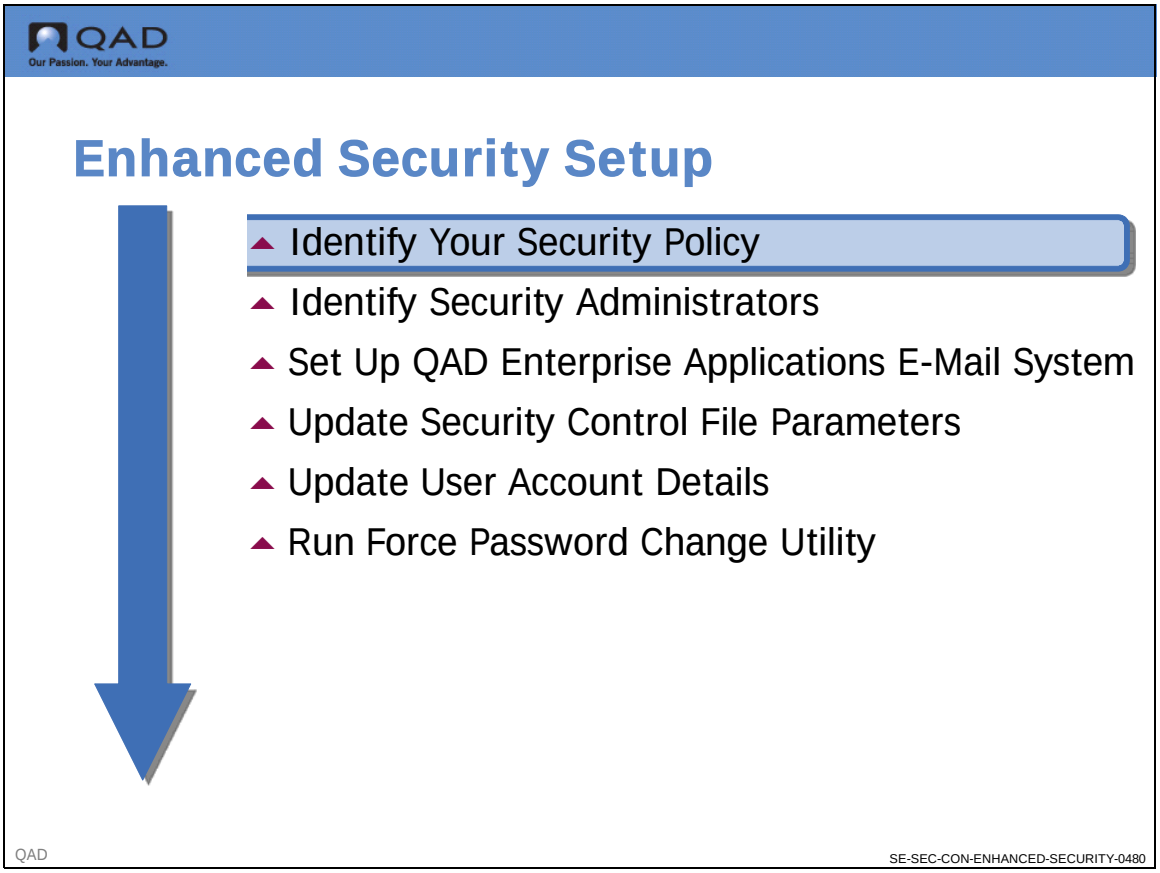
In the area of Intrusion Detection, QAD enhanced the ability to identify when unauthorized users have attempted to access the system

Enhanced Security Setup Steps

What do you need to do within the system to enable these capabilities?

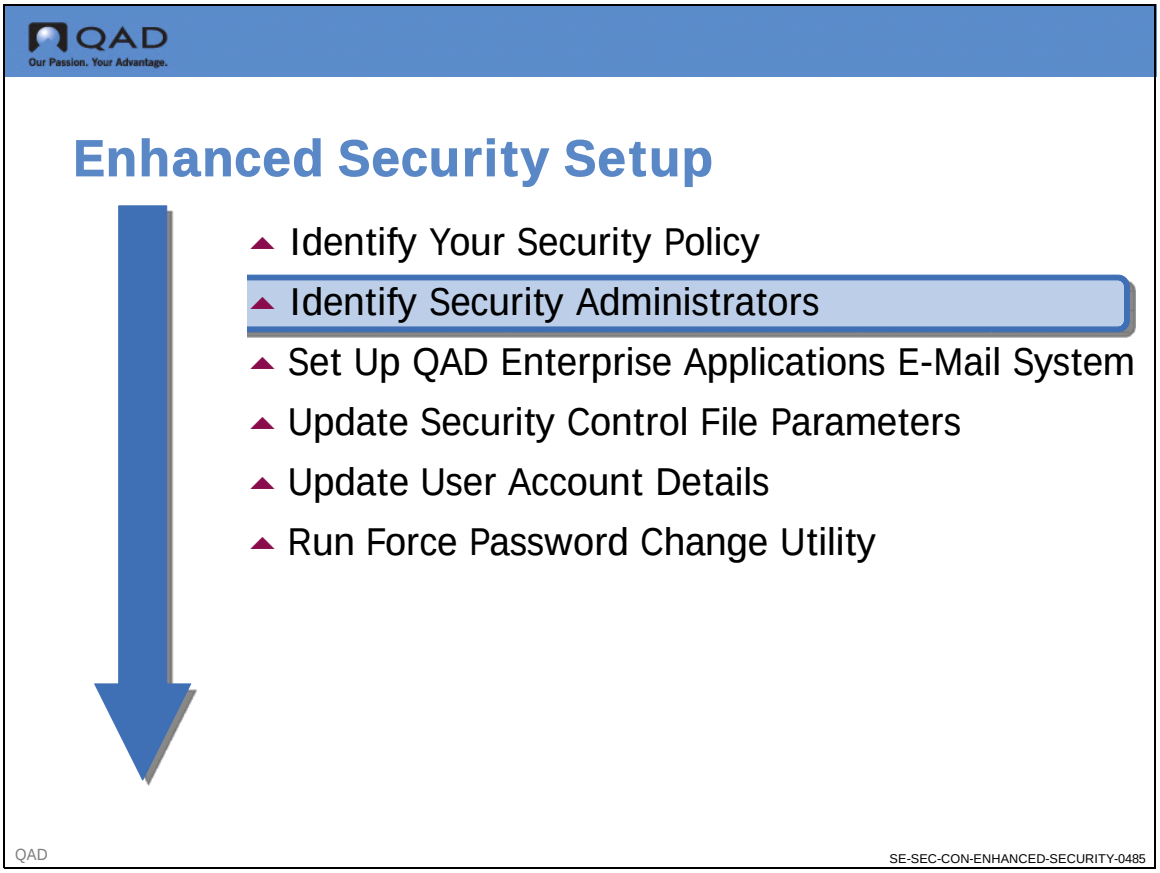
- Identify your security policy
- Identify security administrators
- Define e-mail system
- Update security control file parameters
- Update user account details
- Run Force Password Change Utility

Identify Your Security Policy



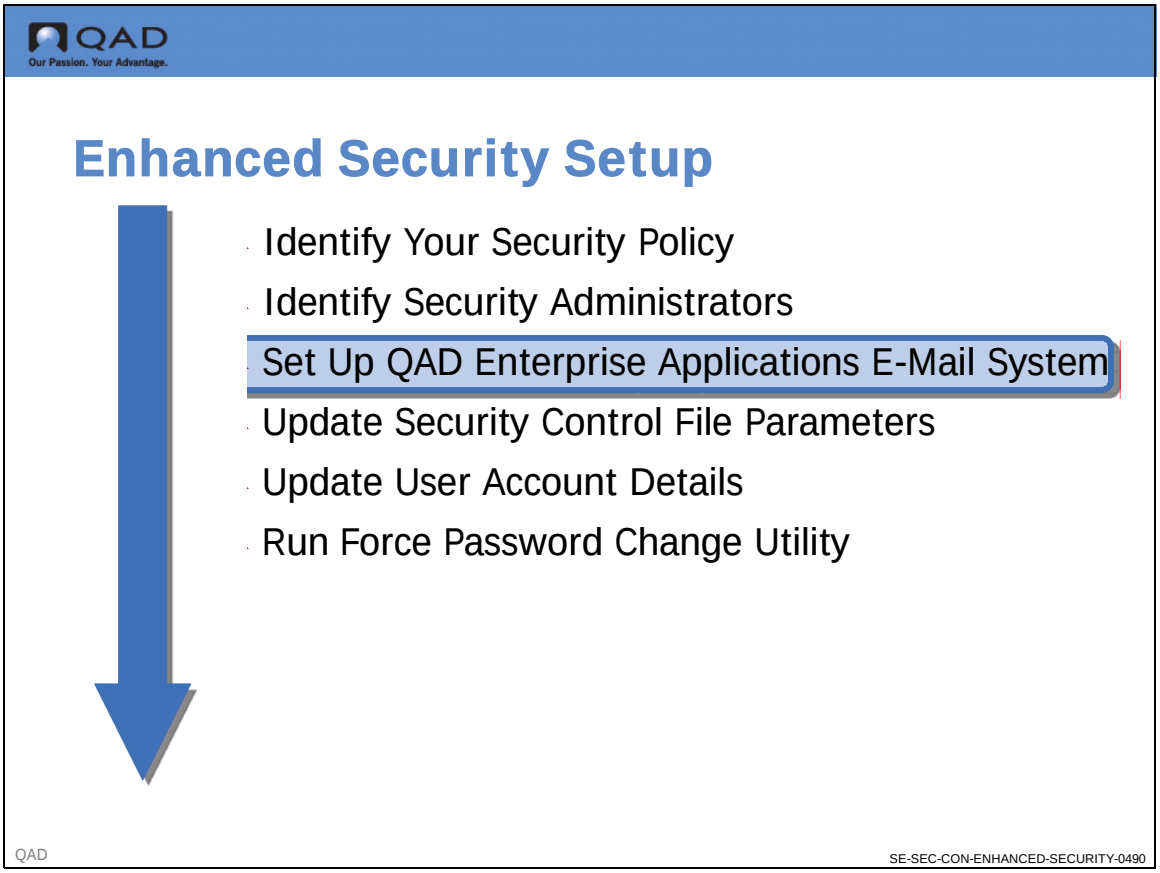
The password should be at least 8 characters in length and contain a mixture of numeric and non-numeric characters.

Identify Security Administrators



You need to identify an administrative group and nominate trusted individuals within your IS area to that group.

Set Up QAD Enterprise Applications E-Mail System

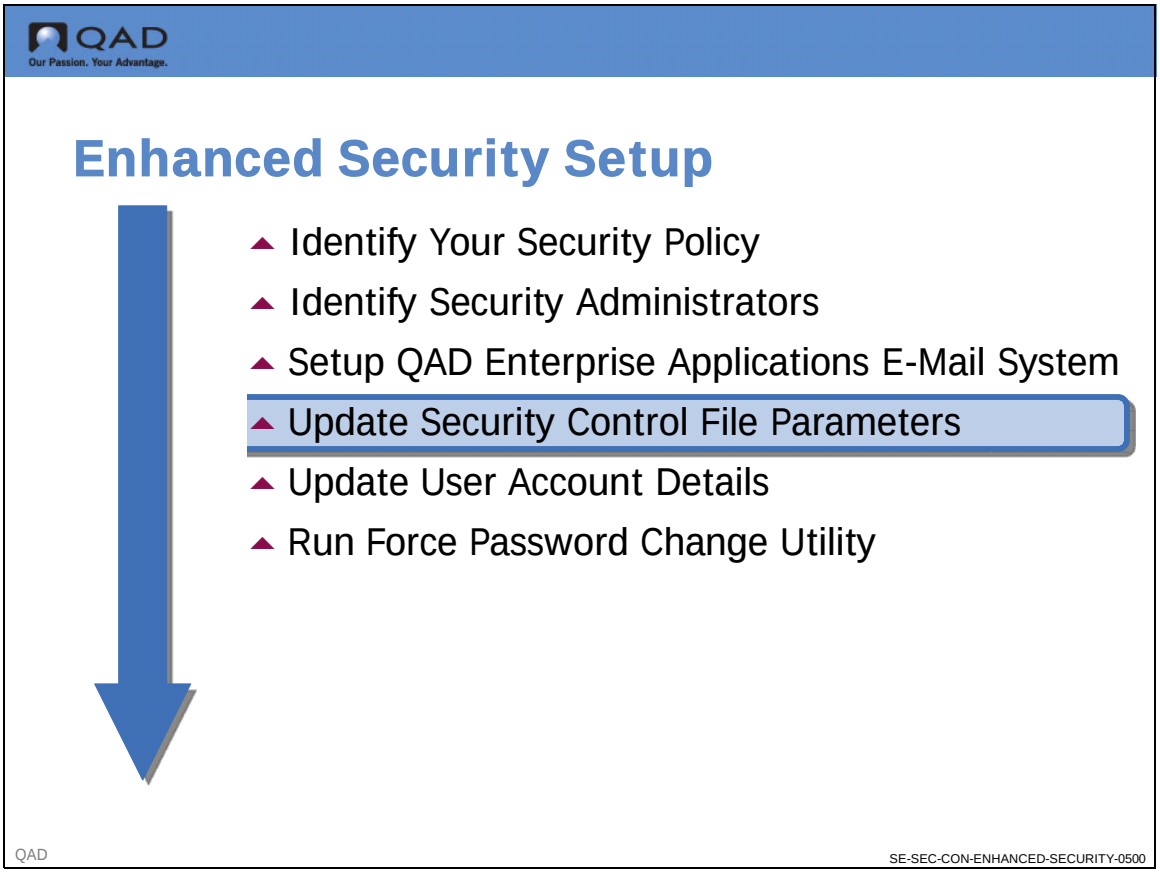


The next step is setting up the QAD Enterprise Applications e-mail system; e-mail is a cornerstone of the solution. It can operate without e-mail setup, but many of its capabilities will not be fully utilized. For example, security alert functions, will only generate messages to Admin Group members with e-mail accounts.

The Automatic Password Generation with e-mail security settings requires that all QAD Enterprise Applications users have a valid e-mail account.

E-mail system setup is described in QAD Enterprise Applications administrator documentation.

Update Security Control File Parameters

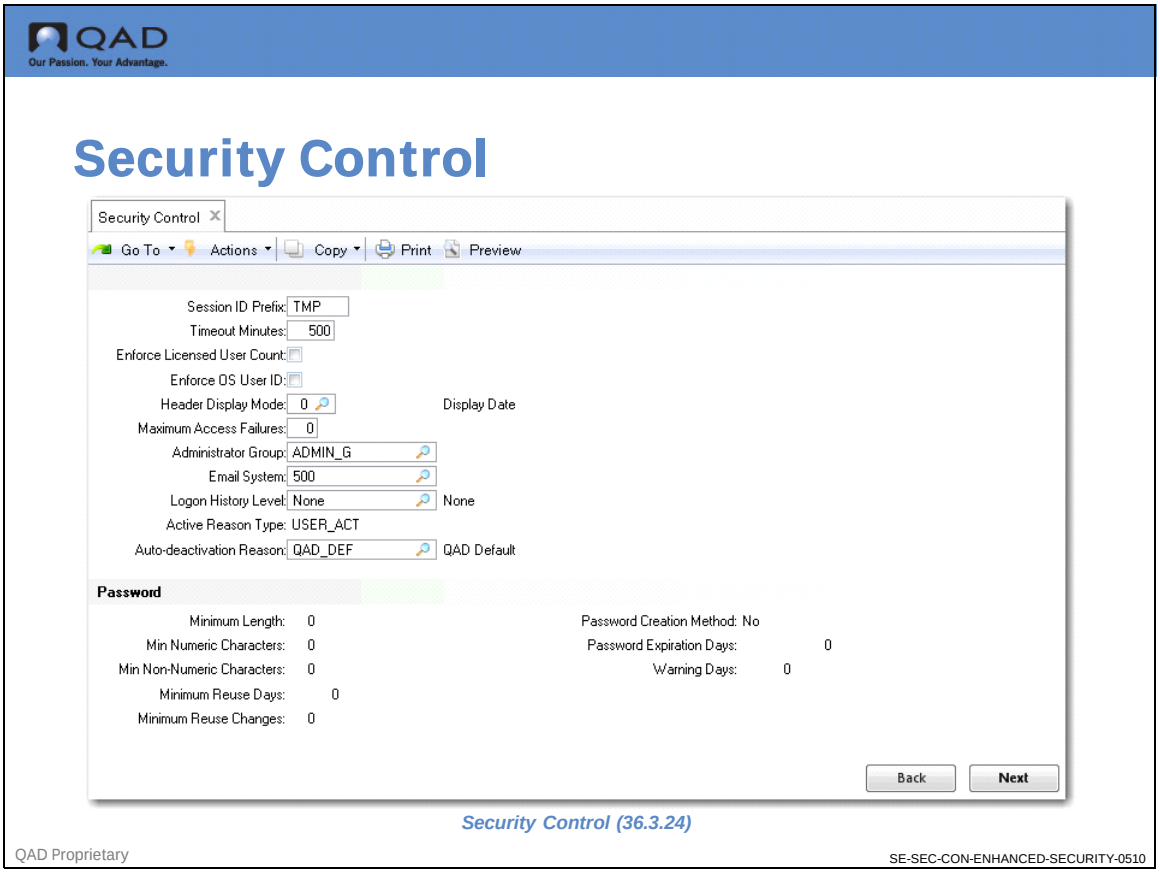


The next step is to update the security control file parameters. Within the security control file are three basic categories of parameters where QAD has made changes:

- Control parameters
- Password complexity parameters
- Password creation and aging parameters

Below is the desktop screen that shows the Security Control file.

Security Control (36.3.24)



Control Parameters

Header Display Mode (Optional). Replace the date display in the top left hand corner of the screen with the user's logon id or domain. This characteristic relates mostly to the character versions of QAD Enterprise Applications.

Maximum Access Failures. The number of consecutive failed logon attempts before a user's account is deactivated.

Administrator Group. Contains individuals to contact when significant security events occur on the system. It is a standard QAD Enterprise Applications user group. Individuals are assigned to that group as you would in QAD Enterprise Applications

E-mail System. Identifies a particular e-mail system.

Logon History Level. Enables a log file that records attempts by users to logon to the system. The product offer three levels of logging. No Logging logs no information to this file. Only Failed Logon Attempts logs failed logon attempts to the file. Log All Logon Attempts. History can be reported from this logon information.

Active Reason Type. The reason type associated with reason codes entered for user account activation and deactivation.

Auto Deactivation Reason. This is the code that the system uses when the system deactivates a user account (for example, the deactivation that occurs when a user exceeds their maximum permissible logon attempts). This is the deactivation reason code that is applied against that user's information and logged. The auto deactivation reason codes are set up in the standard Reason Code Maintenance within the system, therefore, you need an active reason type code to identify the reason codes associated with the Active flag.

Password Complexity Parameters

Minimum Length. The minimum number of characters over 8.

Min Numeric Characters. The minimum number of numeric characters

Min Non-Numeric Characters. The minimum number of non-numeric characters

Minimum Reuse Days. This is the number of days a user must wait before a password can be reused. If you set Minimum Reuse Days to 20 and a user had password XYZ, the user cannot use password XYZ until at least 20 days have passed.

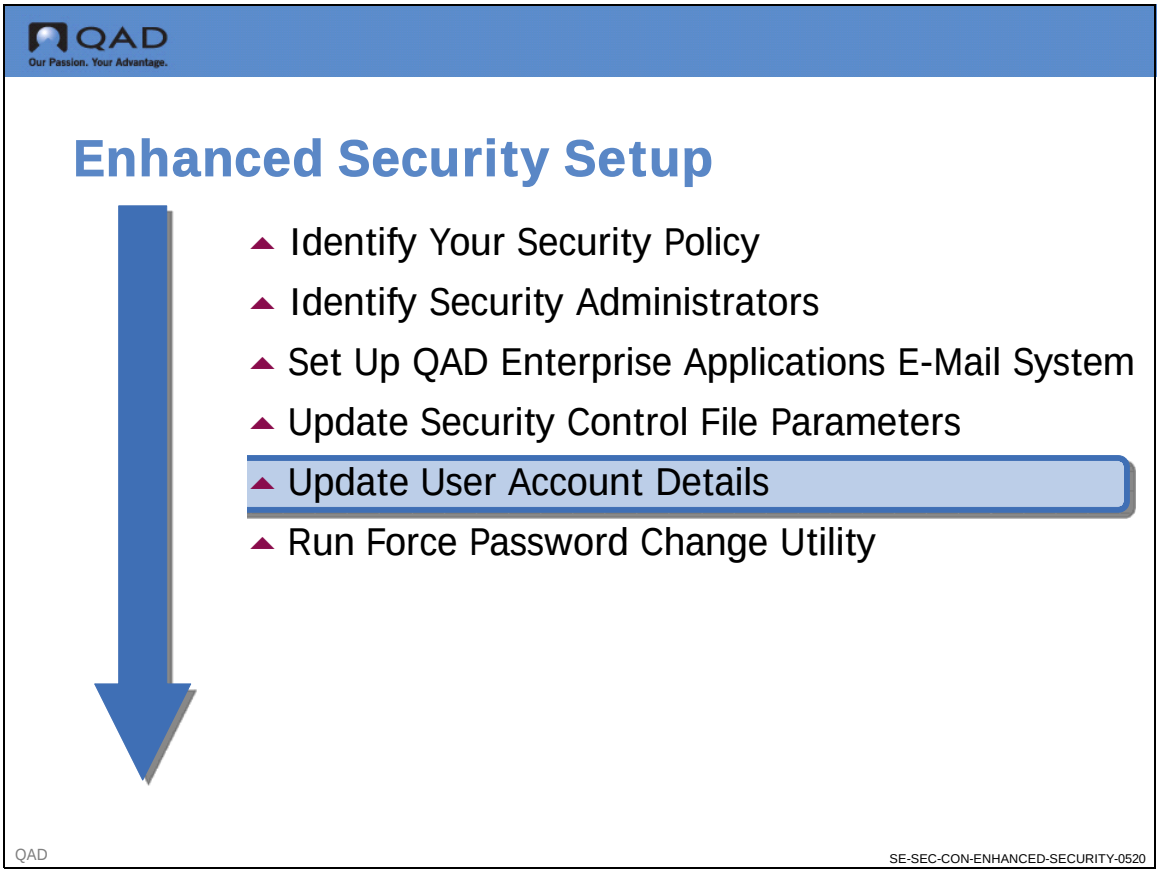
Minimum Reuse Changes. Indicates the number of password changes required before a password can be reused. For example, assume that 10 password changes must have occurred between reuse of a password. If you have password XYZ today, it must be changed 10 times before it can be used again.

Password Expiration Days. The number of days that the user can use the same password before being forced to change. Setting Password Expiration Days at 30 means a user's password ages every 30 days and they must change it.

Warning Days. The number of days before password expiration that the user is warned of the pending expiration. It can be set any number of days.

Note Minimum Reuse Days and Minimum Reuse Changes operate together.

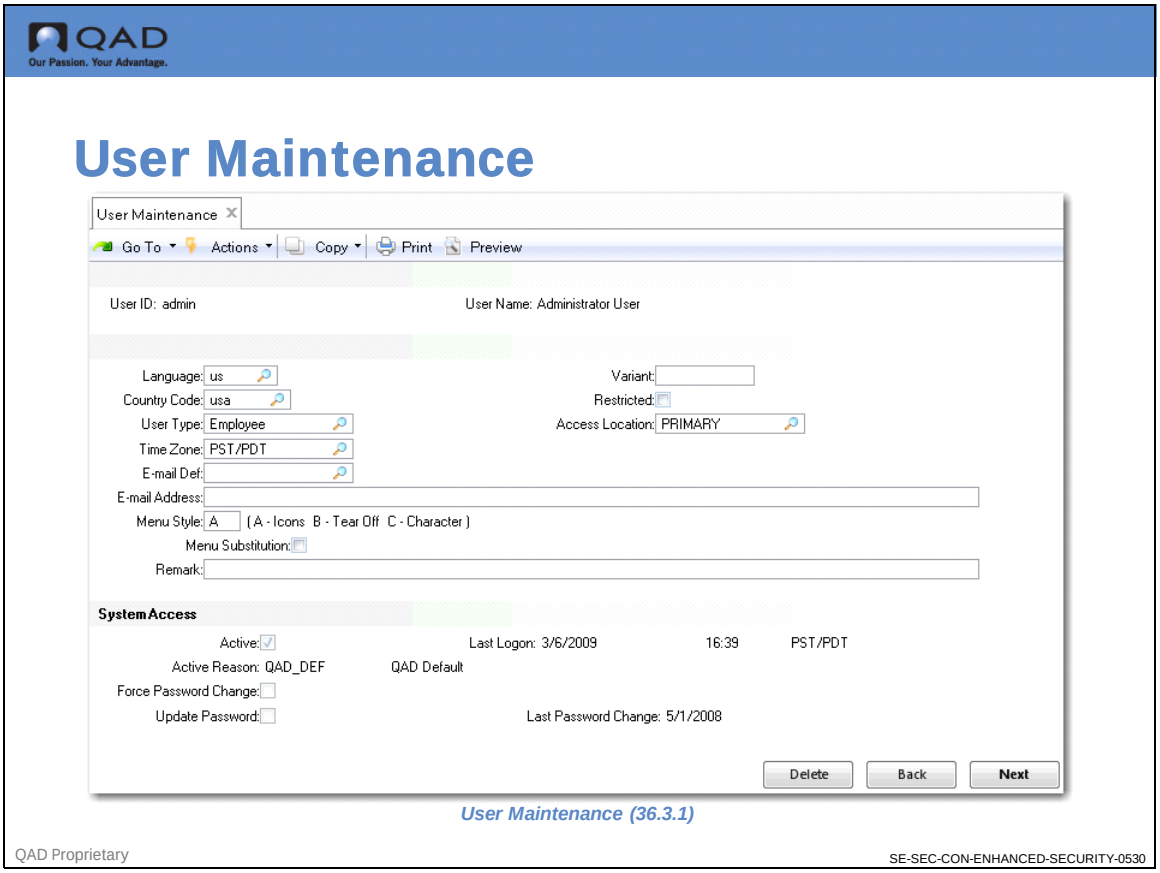
Update User Account Details



The next step is updating the user account details. One fundamental change is that user accounts can no longer be deleted on the system. Accounts can be deactivated, this means they cannot be used to logon to QAD Enterprise Applications.

Deactivation can be manual through User Maintenance or automatic as a result of a user exceeding the permissible number of failed consecutive logon attempts.

User Maintenance (36.3.1)



User Maintenance (36.3.1)

Remark. A freeform comment to associate with this user.

Active. Indicates whether this user account can be used to log on to the system. This identifies whether the user is Active or not.

Active Reason. The reason code associated with the last change of the users active flag. Whenever there is a change to the Active status flag, a reason code must be logged of the type that has been identified in the Security Control file.

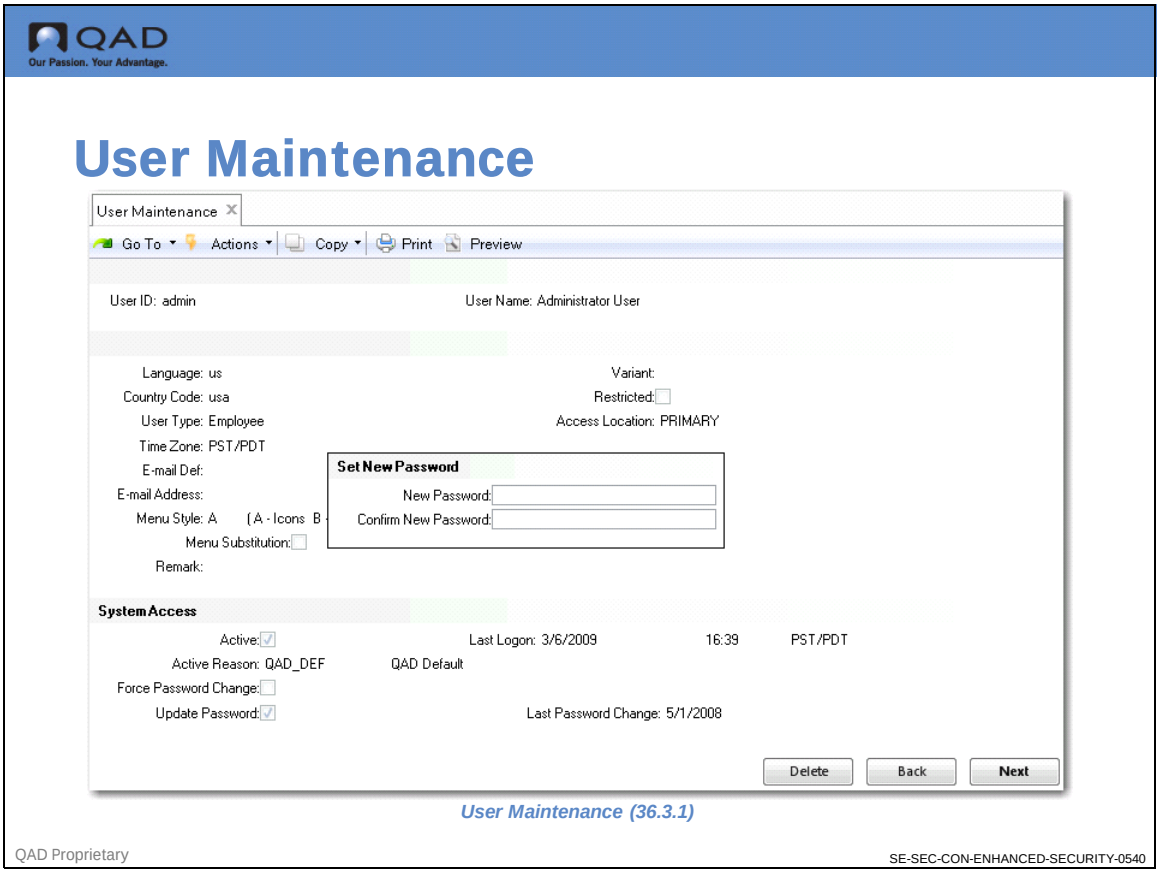
Force Password Change. Enables the administrator to force the user to change their password the next time they log on. This might be necessary if there has been a security breach or if someone's password has been compromised.

Last Logon. Identifies the last successful logon date and time for the user. This can help to determine where a user's account might have been used without their knowledge.

Update Password. Identifies whether the administrator wishes to change the user's password.

There is also a utility that enables the mass setting of the Force Password Change flag.

User Maintenance (36.3.1) - Frame 2



User Maintenance (36.3.1)

Administrator Selects Update Password

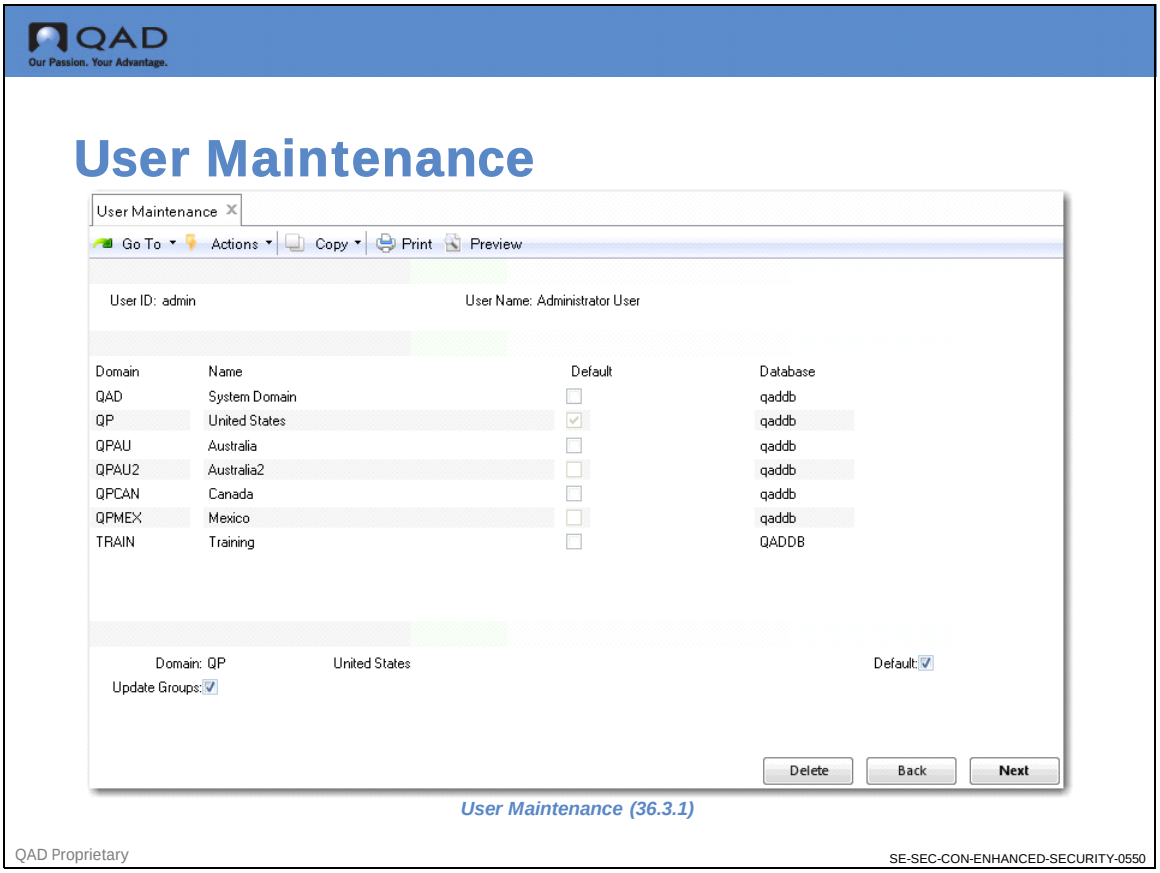
The next flag is allows the administrator to select update of the password.

Whenever a user's password is being updated, the user is asked to enter the password twice. And also outside of the context of User Maintenance, the user is required to enter their current password before changing the password.

User Group Maintenance is not completed on the main screen. Because user groups are domain specific, they are maintained from a screen attached to the domain setup screen for the user. User Groups are not maintained through a comma-separated string.

On the domain screen for a given domain that has been identified for a user, there is a flag at the bottom that identifies whether you wish to update the groups for that domain for that user.

User Maintenance (36.3.1) - Frame 3



User Maintenance (36.3.1)

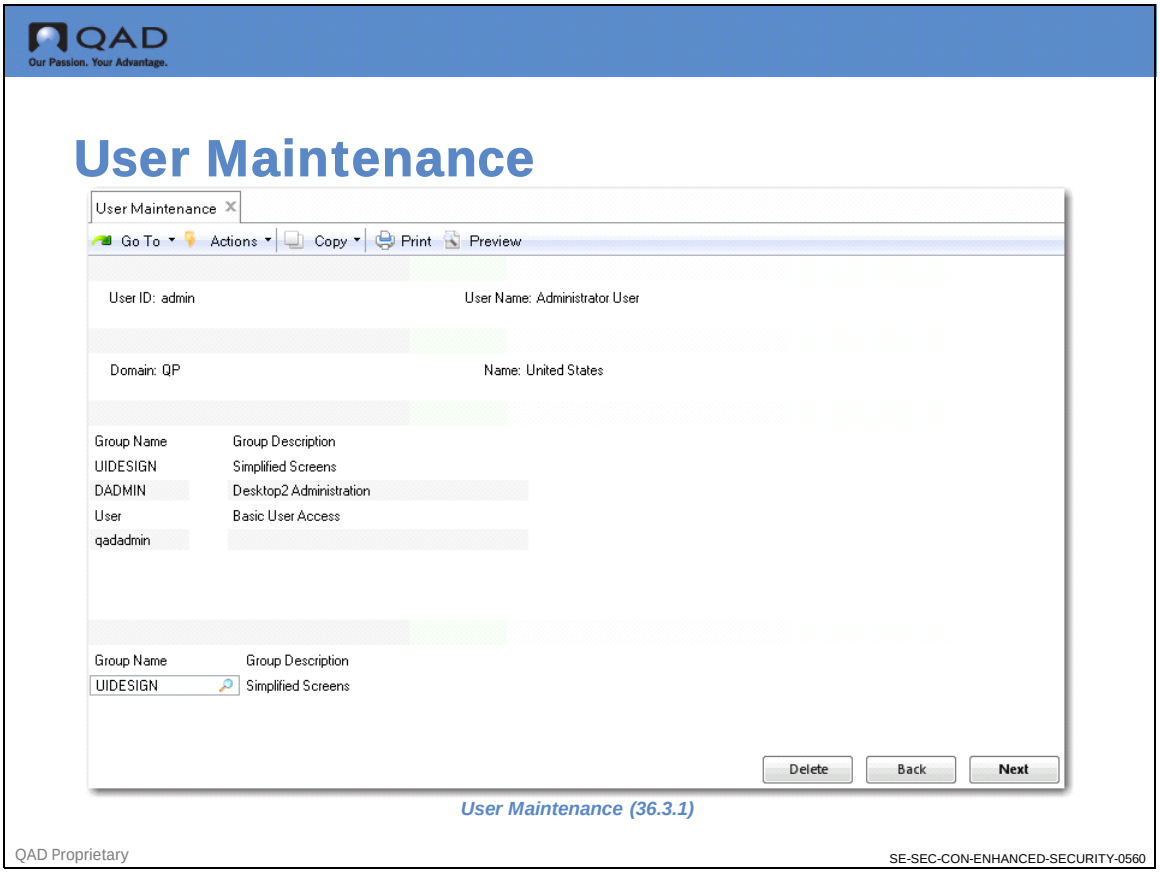
QAD Proprietary

SE-SEC-CON-ENHANCED-SECURITY-0550

Administrator Selects Update Groups

After selecting that flag, you come to the screen where you are able to associate groups with the user.

User Maintenance (36.3.1) - Frame 4



User Maintenance (36.3.1)

Adding Groups To User Domains

Rather than maintaining a comma separated string and no effective validation occurring against those group names, you now enter the group names through this frame, and they are validated.

User Password Maintenance

The only updatable data in the User Maintenance screen is the user's password. Previously it was possible for someone with access to User Password Maintenance to change the user's name as well.

The User Password Maintenance screen now, mimics the exact form of the standard User Maintenance screen.

User Group Maintenance

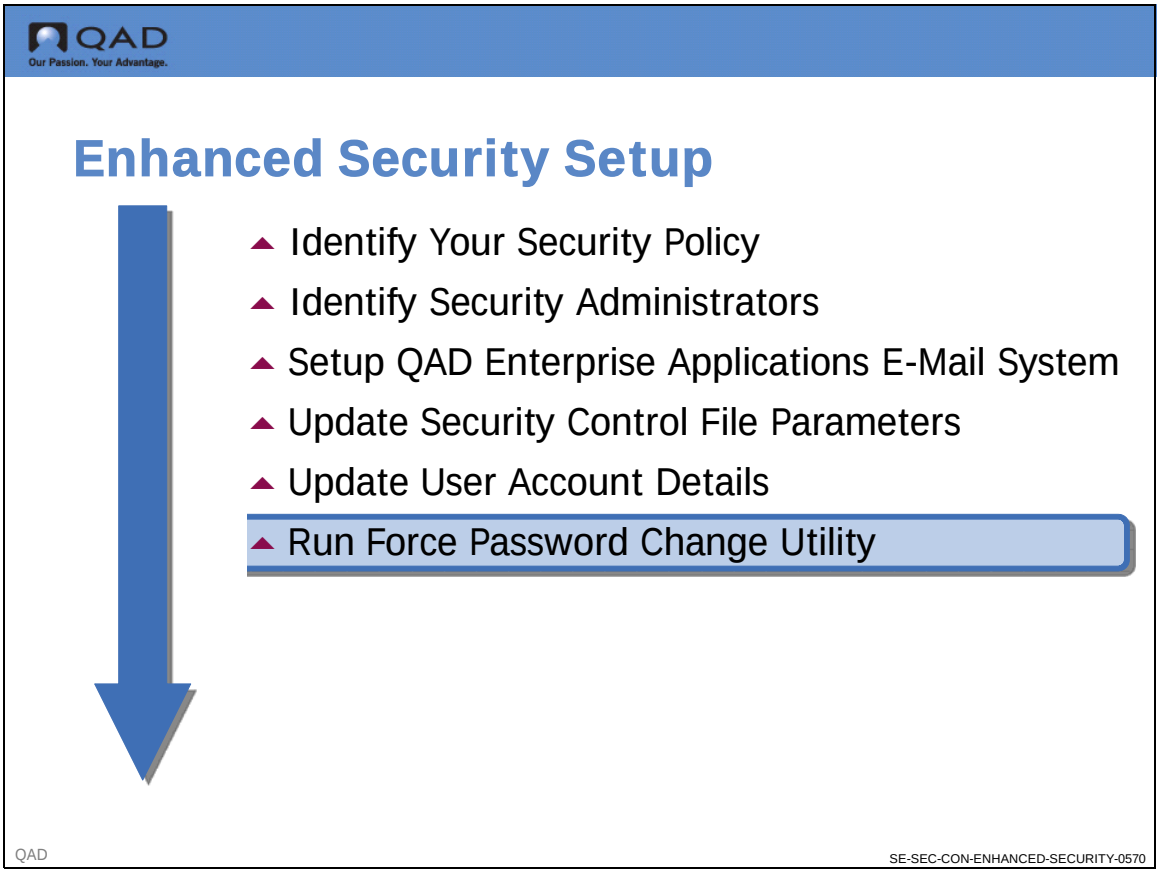
User Group Maintenance provides the following functionality:

- Enables the definition of user groups
- Enables the association of user accounts with those defined groups
- Defined user groups are now used to validate groups when they are entered in:
  - Menu Security Maintenance (36.3.10)
  - Site Security Maintenance (36.3.15)
  - GL Account Security Maintenance (36.3.16)

- Inventory Movement Code Security (36.3.17)

Previously, groups did not exist in a distinct table, and there was nothing to validate against. QAD created a group table and the ability to define the groups, and then to associate user accounts with the groups. You have two ways to associate users with groups: Through user maintenance, whereby you associate the groups with the user, or through group maintenance, where you associate users with groups.

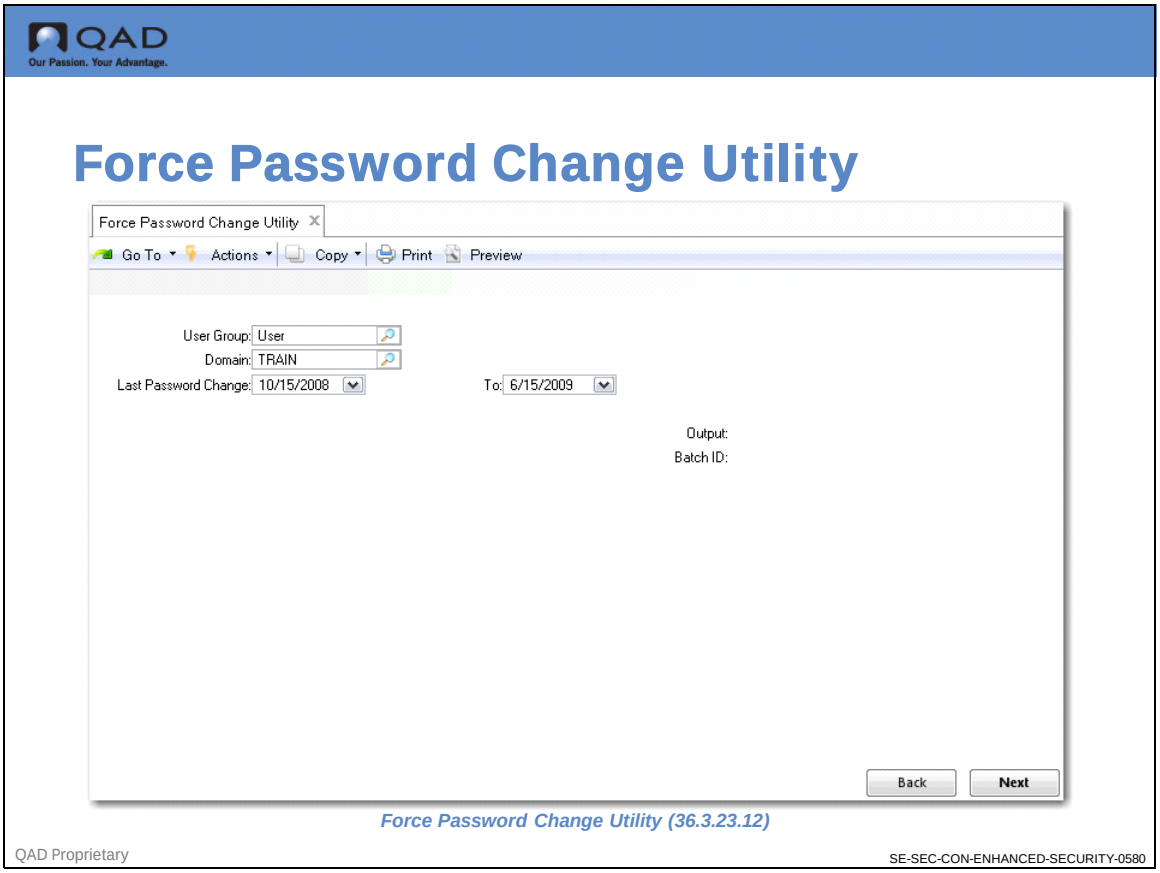
Run Force Password Change Utility



After you have changed all of the necessary parameters, run the Force Password Change utility. This ensures that current users have their passwords generated in agreement with the new password policies.

This utility and allows for the immediate expirations of passwords for a number of users. Any currently logged on users are unaffected until the next time they log on to the system. Users selected by the utility are forced to change their password as part of the next logon.

Force Password Change Utility (36.3.23.12)



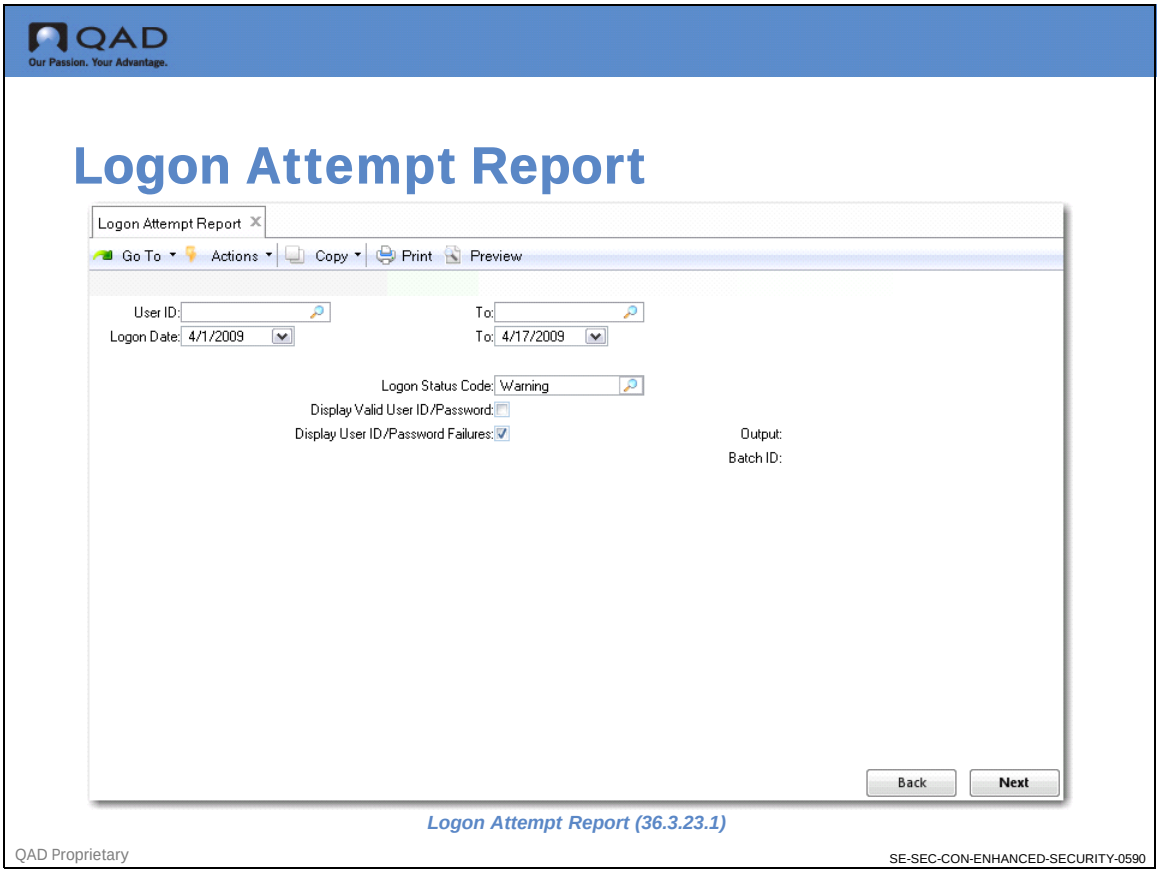
Force Password Change Utility (36.3.23.12)

QAD recommends that this function be run after changing security control settings that affect user passwords. Run this utility is when you believe that there has been a security breach on your system or some attempt to subvert security on your system.

If you leave the User Group value blank, the utility runs for all users. You can limit the Force Password Change to passwords last changed within a particular date range.

For example, you may not want to expire people's passwords who have changed them within the last week, but you might want to force anybody who has not changed their password in two months.

Logon Attempt Report (36.3.23.1)



Logon Attempt Report (36.3.23.1)

Selection Criteria

Logon Status Code. When a user logon is attempted, a code is generated by the system and written to the log file indicating the success/failure and any special conditions or circumstances surrounding the attempt. This report can be generated to only report for a single code. An example might be to only report for Status Code: Deac-Usr this would indicate if attempts were made to logon to the system with a deactivated user account.

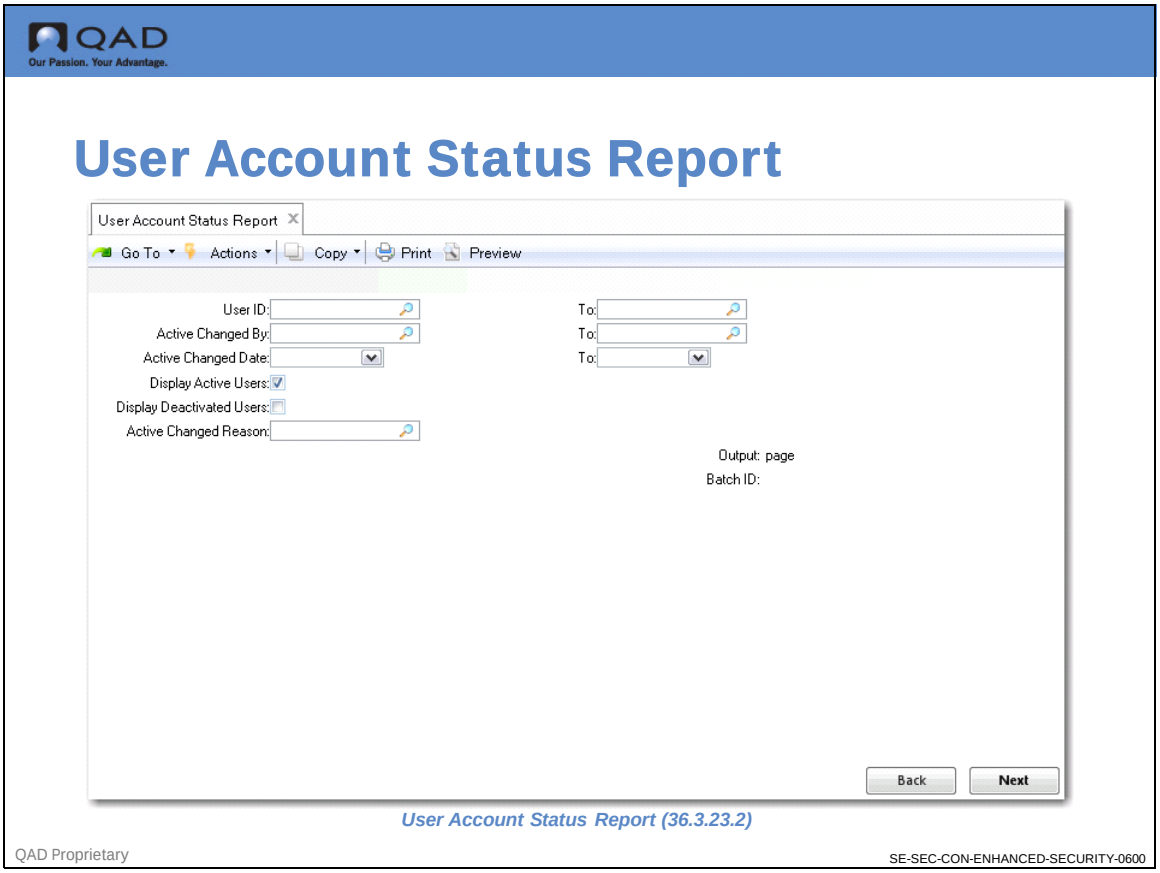
Display Valid User ID/Password. Enter Yes to include successful log-in attempts. Otherwise, enter No. This produces output only if the logon history level in the security control file is set to All. To display all log-in attempts, set this field and Display User ID/Password Failures to Yes.

Display User ID/Password Failures. Set this to Yes to display failed logon attempts. This will produce output only if the logon history level in the Security Control file is set to other than None.

You can run the Logon Attempt Report for a range of user IDs, a range of logon dates, and a range of logon status codes. You might only want to report for those logon status codes that perhaps are of a failed nature.

Output. This is generated from desktop. You have User ID, User Name, the date and time of the logon attempt, whether a valid user ID password was offered during that logon attempt, and the outcome of the logon attempt.

User Account Status Report (36.3.23.2)



User Account Status Report (36.3.23.2)

The User Account Status Report provides user account details. The primary filtering for this report is on the user's active status. It is useful for identifying users whose accounts have been deactivated.

A user ID range may be used. There is also Active Changed By range, that logs who changed a user’s active status. You can identify who changed the user to inactive or active. Also the Date range that the user's status was changed.

You can filter by displaying only those users that are active. You can display the current set of active users on the system or deactivated users. And most importantly, you can also identify an active changed reason.

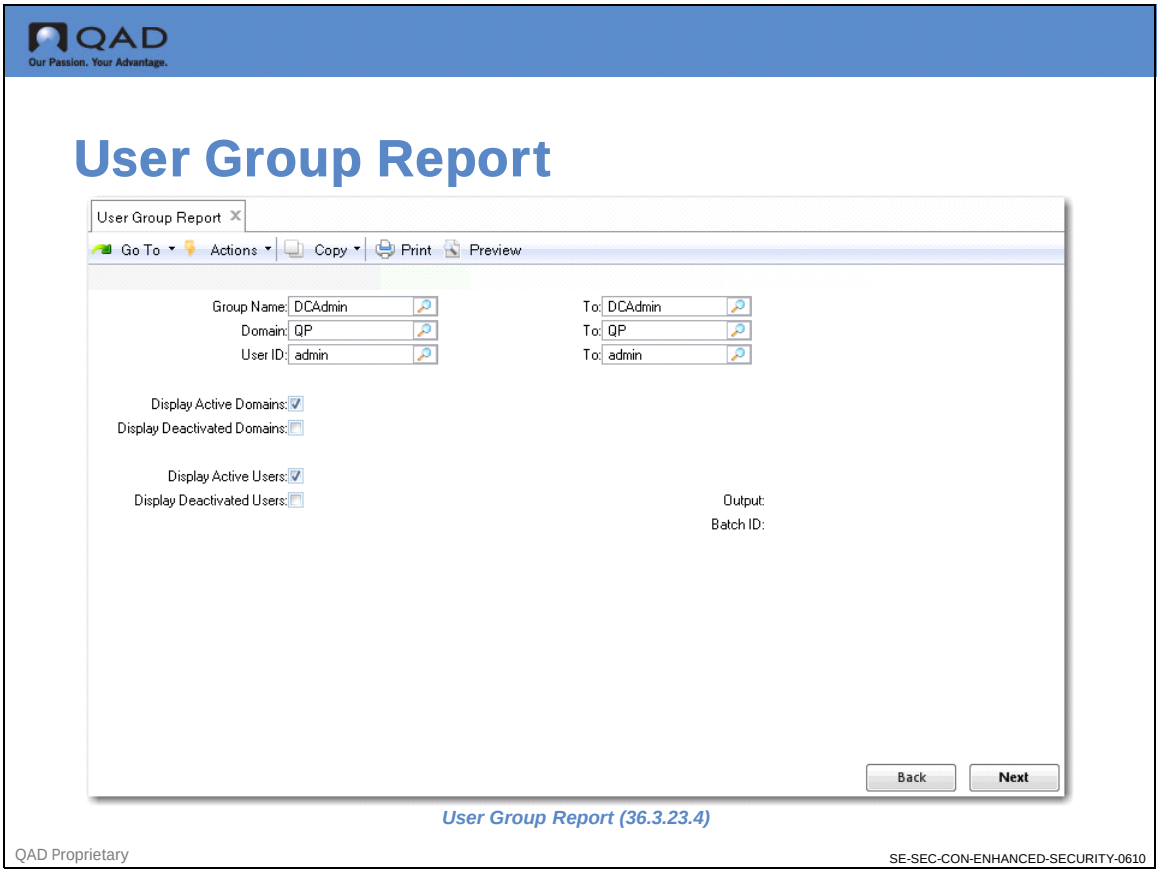
You might want to display those users that have been automatically deactivated by the system. So you would use a Reason code that you have set up in the Security Control file. And that way you can find any users who have been automatically disabled.

As another example, you also might set up an active change reason for people who have recently left the company. Again, you can report on those as well.

When used in conjunction with well-defined user group structures, it identifies which individuals have access to what functional areas in the system.

There is a Group and Domain range in the report (user groups are associated with domains in the system).

User Group Report (36.3.23.4)



User Group Report (36.3.23.4)

The report displays the users associated with a security group in the system.

The report is similar to the User/Group Report and allows for the reporting of users associated with security groups in the system.