

THE SIMPLY HR SOFTWARE COMPANY

Simply Personnel Auditing

SIMPLY PERSONNEL

Version 1.0

Date: 08/03/2008

TABLE OF CONTENTS

1.	INTRODUCTION.....	3
2.	REQUIREMENTS.....	3
3.	INSTALLING THE AUDITING FUNCTIONALITY.....	3
3.1	SQL SCRIPTS.....	3
3.2	COMPLETE AUDITING.....	3
3.3	CUSTOM AUDITING.....	4
3.4	WINDOWS AUTHENTICATION.....	4
4.	REMOVING THE AUDITING FUNCTIONALITY.....	4
5.	REVIEWING THE AUDIT TRAILS.....	4
5.1	SIMPLY PERSONNEL SECURITY.....	4
5.2	SIMPLY ANSWERS.....	4
6.	AUDITING LIMITATIONS.....	5
6.1	DOCUMENTS.....	5
6.2	NOTES FIELDS.....	5

1. INTRODUCTION

This document details the instructions necessary to install and use the auditing functionality of Simply Personnel.

These instructions will explain how to implement auditing within Simply Personnel and how to remove it, along with how to review the audit trails using the Simply Answers query tool.

The way the auditing is implemented means that not only do changes made using Simply Personnel get audited but any changes to the data, regardless of the application or user making the change, will cause the audit trail to be updated. This means any third party product, including SQL Server itself, that updates the data will be audited.

2. REQUIREMENTS

The Simply Personnel auditing functionality is **only** available with the SQL Server implementation and not the Microsoft Access database. The auditing is handled directly by SQL Server itself and the Access database does not provide this level of functionality.

To use auditing you will need one of the following installed and configured to run with Simply Personnel:

- SQL Server 7.0 with service pack 3 or later installed.
- SQL Server 2000.
- SQL Server 2005.
- SQL Express

3. INSTALLING THE AUDITING FUNCTIONALITY

3.1 SQL Scripts

The auditing works by using SQL triggers on the Simply Personnel database tables and fields. These triggers detect when data is inserted, updated or deleted and write the changes, along with who made the change, the application used and the date and time it was done, to the audit tables within the Simply Personnel database.

These triggers are created using the scripts in the Auditing folder from the Simply Personnel SQL Server scripts file. This file is the one available on the downloads page on the Simply Personnel website.

The installed triggers will work in conjunction with any user created triggers on the database tables. If the data is changed then all triggers on the affected fields will be executed, not just the auditing ones.

3.2 Complete Auditing

To audit changes to every table and field within the Simply Personnel database, run the **Audit_All.sql** script in the SQL Server Management Studio or Query Analyzer. This will add the insert, update and delete triggers against every field and cause every change to be audited.

3.3 Custom Auditing

The Auditing SQL script folder contains a number of subdirectories that will allow you to install triggers against selected database tables. For example, if you just want to audit the changes to employee data, run all of the scripts in the Personnel\Employee folder. This means users can make changes to other tables but the auditing will only occur when employee data is changed.

3.4 Windows Authentication

In order to accurately audit who changed the data, the ODBC connection to the Simply Personnel database will have to be changed to use Windows Authentication instead of SQL Server Authentication.

The reason for this is that by default the ODBC will use SQL Server Authentication and the username 'Personnel'. This will cause the audit trail to report that it was this user that changed the data. By switching to Windows Authentication the audit trail will report the Windows username of the person that changed the data.

To use Windows Authorisation, add the Windows usernames into security logins in SQL Server. Give the logins full permissions against just the Personnel database and then reconfigure the ODBC settings on the client computers to use Windows Authentication instead of SQL Server Authentication.

4. REMOVING THE AUDITING FUNCTIONALITY

To remove the auditing functionality you need to delete the triggers on the database tables. This is done by running the Remove_Auditing.sql script in the SQL Server Management Studio or Query Analyzer.

Open the script and run it against the Personnel database. This script will remove the auditing triggers but leave any user created triggers intact. Once removed, SQL Server will stop updating the audit tables with data changes.

5. REVIEWING THE AUDIT TRAILS

5.1 Simply Personnel Security

Users of Simply Personnel can be prevented from viewing the audit trails by using their Access Profile.

Run Simply Personnel and select the **Tables** → **Security** → **Access Profile Maintenance** menu option. Update the user's profile and you will see the "**Restrict Audit Reporting (SQL Server only)**" option in the **Licensed Products** group at the bottom of the screen.

Left click on the box here to display a tick mark and the user will no longer be able to view the audit trails. Clear the tick mark and the user will be able to view the audit trails again.

Please note that the user's other security settings will not be applicable when viewing the audit trails. Users will be able to see **all** of the audit trails and not just the audit trails for the screens and employees they are permitted to view. For this reason only the senior administrators of Simply Personnel should have the auditing enabled.

5.2 Simply Answers

To view the audit trails you need to use Simply Answers. If your access profile permits the audit trails to be viewed then there will be a new option available in the tree structure on the left of Simply Answers called Auditing.

Expanding this option will display the fields available on the main auditing table and the fields also available in the linked data table. The description of each of these fields is below.

Field	Description
Database	The name of the database that was updated, normally 'Personnel'.
Table Name	The name of the table that was updated.
Table Schema	The table schema used by SQL Server.
Audit Action ID	Identifies how the data was changed, 1 – Update, 2 – Insert, 3 – Delete
Host Name	The computer that was used to modify the data.
Application Name	The name of the application that modified the data.
Modified By	The Windows username that was used to modify the data.
Modified Date	The date the data was changed.
Affected Rows	The numbers of rows in the table affected by the change.

Field	Description
Data ID	A unique ID number for the data.
Primary Key Data	The primary key on the database table.
Column Name	The name of the database field that was altered.
New Value	The value the data was changed to.
Old Value	The value the data was changed from.

6. AUDITING LIMITATIONS

6.1 Documents

There is a limitation with the auditing functionality related to embedded and linked documents. SQL Server is unable to audit changes to the actual documents themselves as it cannot monitor the physical contents of the documents.

Changes to the document's other information in Simply Personnel, such as group, date created and notes can be detected but not the document's content. Neither Simply Personnel or SQL Server can detect changes in the binary data that is either stored in the database or located elsewhere on the computer or network.

6.2 Notes Fields

Due to the way SQL Server stores notes fields, it is possible for the auditing to report that these have changed when they actually haven't. What is happening is that when the database record is saved the underlying storage of the text changes although the actual text may not have. It is this change that SQL Server detects and audits, not the text itself. If the text has changed though then this will be reported.