SIEMENS

DESIGO™ INSIGHT V2.35 – Pharma solution SP1

System description

CM110515en_02
21.05.2007

Building Technologies
HVAC Products

Siemens Switzerland Ltd.
Building Technologies Group
International Headquarters
Gubelstrasse 22
CH-6301 Zug
Tel. +41 41-724 24 24
Fax +41 41-724 35 22
www.sbt.siemens.com

Table of contents

1 General description

1.1 Introduction

Aim of this document

This document describes the basic functionality of the DESIGO™ INSIGHT V2.35 – Pharma Solution. It is intended for verification of the installed end product at the customer's facility.

The solution described in this document provides the following functionality as add-ons to the basic functions of DESIGO™ INSIGHT V2.35 SP2.

- Traceability of all GxP-critical data
- Searching and reporting within the audit trail or archived data
- Security backup for databases
- Checksum secured archiving for a defined data retention period

1.2 System topology

The diagram below depicts the recommended topology for the DESIGO™ INSIGHT V2.35 - Pharma Solution. Other variations of this topology are possible, but should be checked with the responsible country product manager and the HQ Pharma Center of Competence.

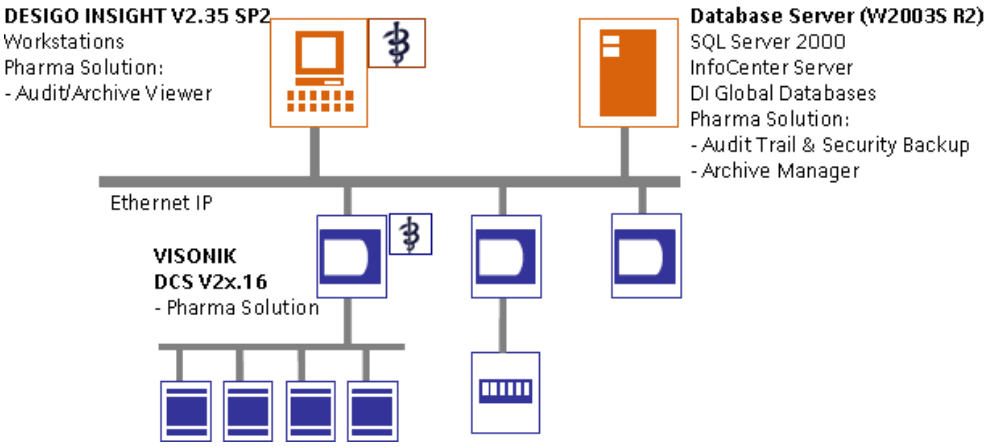

Figure 1: Example of a network topology.

The SQL server contains both the global DESIGO™ INSIGHT databases and the Pharma Solution modules for the audit trail, archiving and backup features. Each DESIGO™ INSIGHT workstation must be registered with the Pharma Solution audit trail. The Audit/Archive Viewer application can either be installed on a workstation or on the server.

This topology is recommended for use with the InfoCenter® Suite monitoring system. In which case, the Microsoft SQL Server 2000 would additionally contain the InfoCenter® server with its databases.

The InfoCenter® client applications (Administrator and Report Manager) can then be installed on any DESIGO™ INSIGHT workstations.

The Audit Trail, Backup and Archiving modules of the DESIGO™ INSIGHT V2.35 – Pharma Solution must be installed on the Microsoft SQL Server 2000 machine. The global databases for DESIGO™ INSIGHT must also be installed on this server.

The combined use of DESIGO™ INSIGHT as a workstation and data server together with the Pharma Solution is not recommended for performance reasons.

Warning!

If DIPS and InfoCenter are to be installed together on the same Server, a second license for SQL is required – even though InfoCenter includes an SQL license.

The InfoCenter SQL license is limited for use only with InfoCenter and not for other software that requires SQL Server.

1.3 Prerequisites / System requirements

The following prerequisites apply to the server for the DESIGO™ INSIGHT V2.35 global databases and to the Pharma Solution Audit Trail, Archiving and Backup modules.

- Microsoft Windows 2003 Server R2 (or higher) or
- Microsoft Windows 2000 Server SP4 (or higher)
- Microsoft SQL Server 2000 SP4 (or higher) Standard Edition.
- DESIGO™ INSIGHT V2.35 SP2 data server only – running in Service mode

All DESIGO™ INSIGHT management stations must meet the following requirements:

- DESIGO™ INSIGHT V2.35 SP2 – running in Desktop mode

All PCs where use of the Pharma Solution Archive Manager or Audit/Archive Viewer applications is required must meet the following requirements:

- Microsoft Windows 2000 Professional, Windows XP Professional, Windows Server 2000 family or Windows 2003 Server
- MDAC V2.8 or higher

2 Traceability of all GxP critical data

2.1 Audit trail functionality

A database level Audit Trail on GxP critical data prevents unauthorized attempts at modifiying data in the DESIGO™ INSIGHT V2.35 SP2 log, trend and system databases. The audit trail information is stored within its own database. Actions of certain «automated users» are excluded from the audit trail.

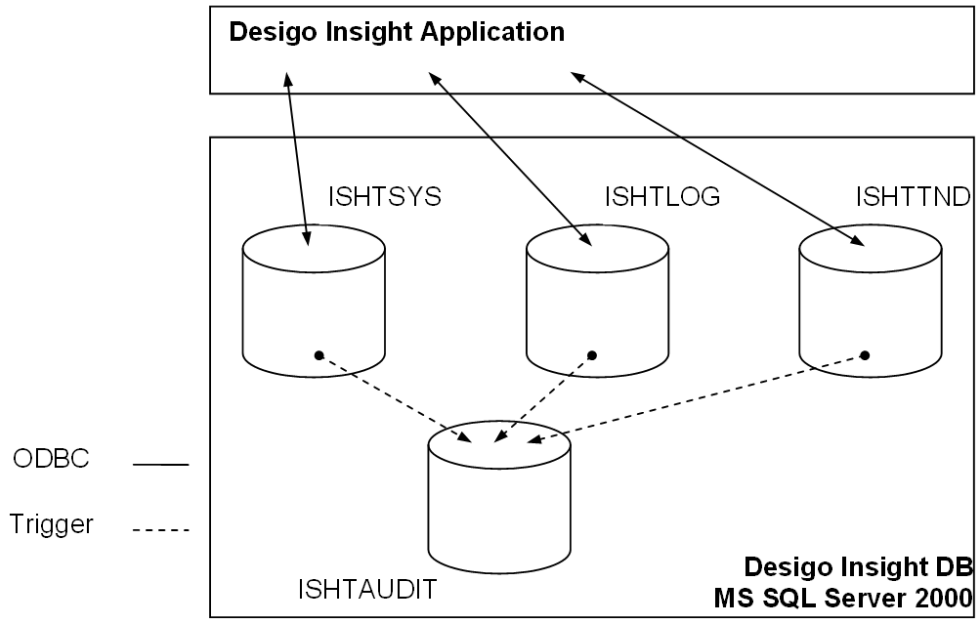

Figure 2: Overview of Audit Trail architecture

2.1.1 Special actions

Exclude “Passwords”

Passwords are not GxP data, so they do not have to be included explicitly in the audit trail. If a password that is stored in a DI database field is added, updated or deleted, a placeholder is added to the «OldValue» or «NewValue» field in the Audit Trail database instead of the actual password.

The placeholder values are:

- INSERT: [OldValue] = NULL,
  [NewValue] = “[New UserPassword inserted]”
- UPDATE: [OldValue] = “[Existing UserPassword modified]”
  [NewValue] = “[Existing UserPassword modified]”
- DELETE: [OldValue] = “[Existing UserPassword deleted]”
  [NewValue] = NULL

2.1.2 Qualification testing

Rationale

Rationale for testing auditing of “INSERT”, “UPDATE”, and “DELETE”, actions:

The test plan for qualifying the correct auditing of “INSERT”, “UPDATE”, and “DELETE” actions is based on the following conditions and conclusion:

- The correct installation of all new DB objects (databases, tables, triggers, etc.) is tested in the IQP. Thereby implying that all triggers necessary to audit “INSERT”, “UPDATE”, and “DELETE” actions on all GxP critical data are known to exist.
- A scripting utility based on a «standard-like» template automatically generates all defined scripts. This utility reads the actual database structure and then uses a template to generate the scripts, during which the triggers necessary for creating an audit trail are installed. The template is applied to each database field, and it implements the specified functionality.

Conclusion

Therefore, the qualification of the audit trail functionality for one table per database is sufficient. This statement is based on the fact that all triggers are generated on the basis of the same template for each database, and that the presence of all necessary triggers has been confirmed in the IQ (see IQP). Additionally, all references to actual database objects are guaranteed to be valid, since the resultant scripts are based on the actual database structure.

2.2 Searching and reporting within the audit trail or archived data

With the Audit / Archive Viewer application it is possible to browse, search and filter data from within the Audit Trail database or any Pharma Solution XML archive file. The application can be used to generate printable audit reports. When viewing archived data, the MD5 checksum is verified and the results are also presented and included in the report.

This application uses either the built-in windows authentication or the standard SQL user authentication to connect with and view the online audit trail database.

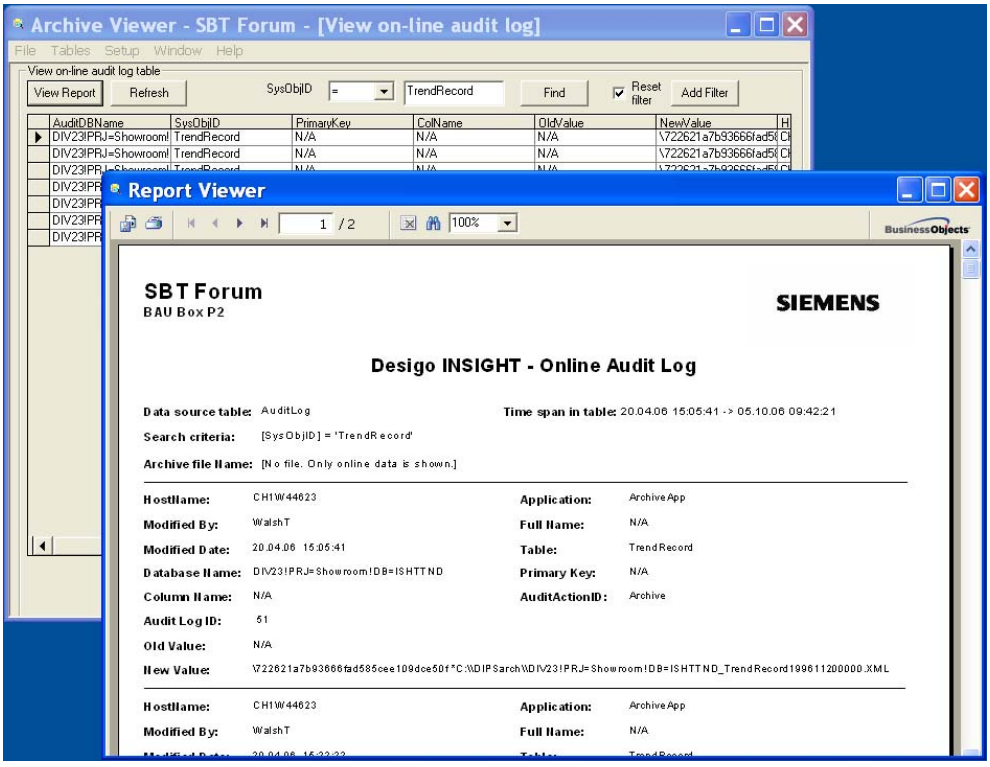

Figure 3: The Audit /Archive Viewer application and an example audit trail report

3 Security backup for databases

The Pharma Solution software automatically creates two backup files for each of the audited DESIGO™ INSIGHT databases (audit, log, trend and system). The backup file names reflect the database name and whether it contains data or transaction log files. The two backup files for the Audit Trail database are:

ISHTAUDIT_DBMedia - Backup filename for the Audit Trail database's data.
ISHTAUDIT_LogMedia - Backup filename for the Audit Trail database's transaction log.

The backup files for the other databases follow the same format, beginning with the short database name as displayed in the DESIGO™ INSIGHT Project Utility.

The DESIGO™ INSIGHT V2.35 – Pharma Solution backs up each transaction log file hourly. A snapshot (copy) of the data file is taken each day and added to the backup file. At the end of each week, these files are cleared and a full backup of each database is performed. Note that the backup data file will grow to at least six times its size at the beginning of the week before being cleared at week's end.

In case of a serious system error, database data collected since the last backup can be rebuilt through the SQL Server using these files. Contact your local Siemens Building Technologies office in this situation.

Warning!

Recommendation:
We strongly recommend configuring database backup locations on separate physical media, i.e. 2nd HardDrive or a network location. Since the backup files are intended to enable recovery of data after a serious system or disk failure, it is important to periodically copy the backup files to offline media, such as tape. In order to set up effective offline system backups, you need to be aware of when these tasks are scheduled to run. You can find this detailed information in the installation guide CM110516_02.

Additional site and project specific procedural controls might be required to manage database backup policies. These must be provided separately and do not form part of this product's deliverables.

4 Data archiving over a given Data Retention Period

The Audit Trail specified above is automatically archived according to the user configurable settings for archiving time and retention period. The archived data is available in a human readable form (XML). This open data format guarantees that the electronic data records will remain accessible during the entire retention period demanded by the industry – often spanning decades. The validity of the data is verifiable by using an MD5 checksum. A status message for the archiving process is written to the audit trail database together with the path and filename of the archive file and its MD5 checksum. There is also a user interface that can be used to manually initiate archiving, if for example a “maintenance” week should be archived seperately.

The XML archiving method can also be applied (optionally) to the DESIGO INSIGHT trends and system activity, offering an open, long term and verifiable alternative to the archiving provided within DESIGO INSIGHT. In this case, the archiving functionality provided by the DESIGO INSIGHT System Configurator must be disabled, because DIPS takes over this functionality.

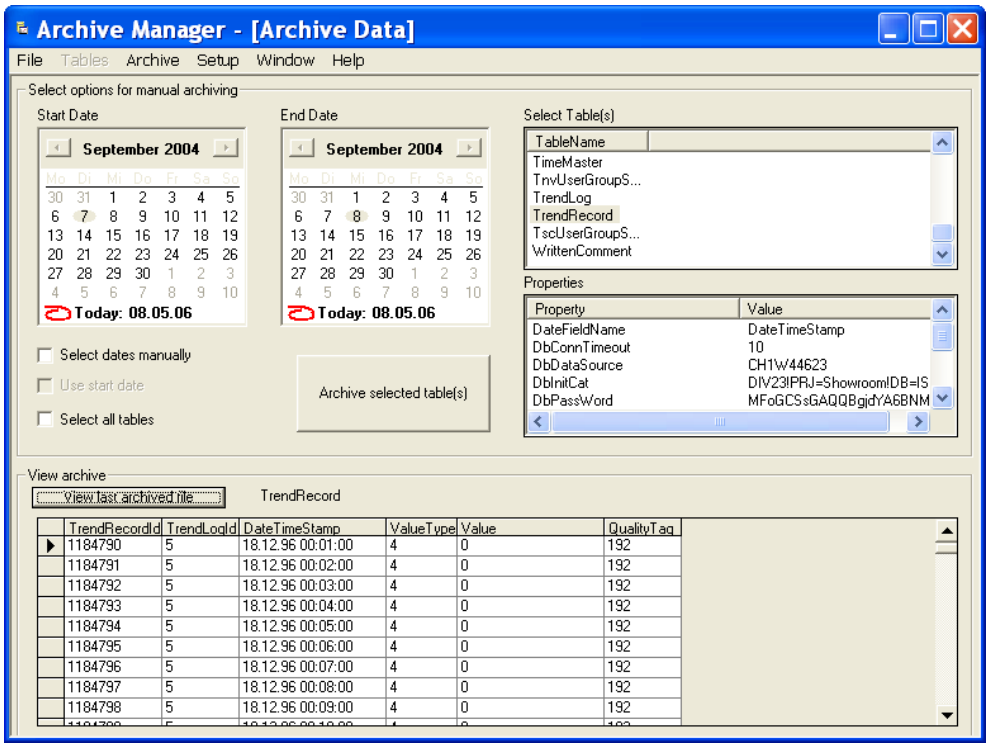

Figure 4: Archive Manager application showing a manual archive action

4.1.1 Special actions

Exclude “Passwords”

The fields; «PWEncryption», «PWSalt» and «PWEncryptionMd5» contained in various tables of the «ISHTSYS» database are not archived by the Archiving application.

Siemens Switzerland Ltd.
Building Technologies Group
International Headquarters
Gubelstrasse 22
CH-6301 Zug
Tel. +41 41-724 24 24
Fax +41 41-724 35 22
www.sbt.siemens.com

10/10