

# ProActive DBA™ Database Auditor™

No-Impact™ Data Usage and Security Auditing for Sybase ASE and Microsoft SQL Server

## Introduction

ProActive DBA Database Auditor from White Sands Technology, Inc. provides 24x7 auditing of all activity in a Sybase ASE or Microsoft SQL Server instance with **No Impact™** on performance.

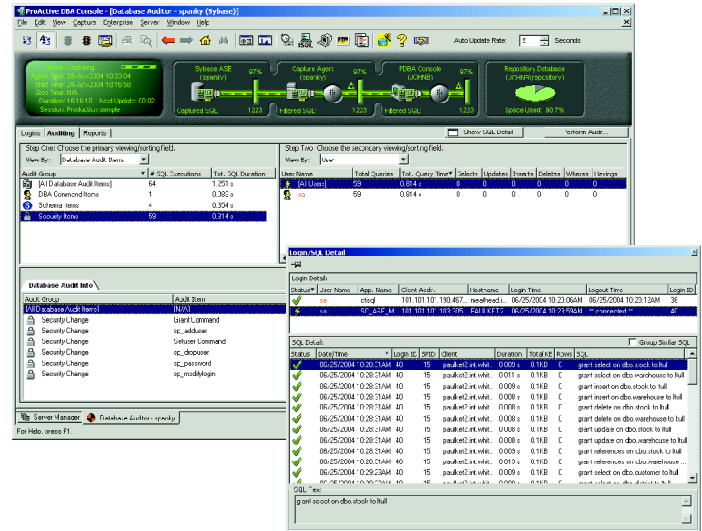
For companies that must comply with the Sarbanes-Oxley, HIPAA or Patriot Acts, **Database Auditor** provides a way to ensure data integrity and accountability for database changes.

Database Auditor shows you:

- **WHO** viewed or changed data;
- **WHEN** the activity occurred;
- **WHAT** data was accessed or modified;
- **WHERE** the activity came from (which client workstation and application)
- **HOW** it was done (direct SQL, stored proc, cursor, etc.)

Auditing solutions built into the database or based on triggers or reading transaction logs can only provide limited information, and usually incur substantial overhead on the monitored server.

Database Auditor is built on the ProActive DBA SQL Capture™ architecture and uses No Impact network sniffing technology to capture all logins,



Monitor accesses to security-related commands, database schema commands and other restricted DBA commands.

logouts and SQL activity between clients and the database server.

DBAs can then analyze captured activity by user, table, application or other criteria to locate audit events of interest.

## Activity Auditing

Database Auditor captures database logins and login attempts in real-time, and shows you the SQL queries that were executed by each login.

You can analyze the captured SQL to view data object accesses and modifications by user, table, application or client address.

See how many times each table and column was referenced in SELECT, UPDATE, INSERT and DELETE statements, and how many times the table/column appeared in WHERE, ORDER BY, GROUP BY and other constructs.

And, you can drill down to see the full, original SQL text, cursor query or stored procedure call (with parameters) that affected a selected table or column, with full details on the query execution (duration, number of rows returned, etc.)

The screenshot shows the ProActive DBA Console interface with the 'Logins' tab selected. It displays a table of login events with columns for User Name, Password, App Name, Client Addr, Hostname, Login Time, Logout Time, Duration, Login ID, SQL Executed, and Tot. SQL Duration. The table shows several login events, including 'sa' and 'sa' users, with details on their login times, durations, and the SQL queries they executed.

View database logins and attempted logins by user, time of day or other criteria.

# ProActive DBA™ Database Auditor™

No-Impact™ Data Usage and Security Auditing for Sybase ASE and Microsoft SQL Server

---

## Track Schema and Security Changes

**Database Auditor** examines client SQL to locate occurrences of the following types of commands:

- Schema changes (ALTER, DROP, etc.)
- Security commands (GRANT, REVOKE, password changes)
- Restricted DBA commands (e.g. DBCC, KILL)

You can view usage of restricted commands and functions by user, application, time of day, etc.

---

## Track Table / Column Usage

**Database Auditor** shows you table and column accesses by user, application, client addresss and other criteria. It shows you how many times each table and column appeared in SELECT lists, WHERE clauses and other SQL constructs, as well as a listing of which tables and columns were not referenced at all.

---

## Purchase Justifications

- See **who** accessed or changed critical data, **what** they did, **when** they did it, **where** the changes were made from and **how** the changes were made
- Monitor accesses to critical data for **Sarbanes-Oxley**, HIPAA, Patriot Act compliance
- Identify accesses to **security**-related functions, **schema** changes and **restricted** DBA commands
- Monitor failed login attempts for **intrusion detection**

---

## Major Product Features

- **No Impact™** 24x7 Network-Based Auditing
- Full Suite of Filtering Options With Wildcards and Pattern-Matching
- Examine Data Usage Patterns by Table, Column, User, Application, Client Address, and More
- Track Schema and Security Changes, DBA Command Usage

- Identify Unused Indexes and Tables
- Save / Load SQL Detail to/from Operating System Flat Files and/or Database Repository
- Summary Reports By User, Application, Client Address, Hostname
- Flexible Capture-Side and Display-Side Filtering
- Schedule 24x7 Continuous Auditing Via GUI and/or Command-Line
- Easiest Installation in the Industry!
- Integration With Other ProActive DBA Products (SQL Capture, Diagnostic Monitor, Visual Space Manager, Database Maintenance Manager, Disaster Recovery Toolset) in a Single Interface

---

## Workstation Requirements

- Windows 2003, XP, 2000, NT 4.0, Me or 98
- Pentium 200MHz or faster CPU
- 128MB or more RAM
- 100MB or more available disk space
- 1024x768 or better display
- Sybase and/or Microsoft client software installed

---

## Database Server Platforms Supported

**Database Auditor** can capture SQL from **any** Sybase ASE or Microsoft SQL Server platform.

Supports **all** Sybase versions 11.0.x through 12.5.x.

Supports **all** Microsoft SQL Server versions 6.0 through 2000.

Capture agents run on Windows, Sun Solaris, IBM AIX, HP-UX, Tru64 Unix and RedHat Linux.



[www.whitesands.com](http://www.whitesands.com)

White Sands Technology, Inc. • 6737 Variel Ave. Suite A • Canoga Park, CA 91303 • 1-818-702-9200 • fax 1-818-702-9100 • [sales@whitesands.com](mailto:sales@whitesands.com)

Copyright © 2004 White Sands Technology, Inc. All rights reserved. ProActive DBA, SQL Capture, No Impact, Database Auditor, Diagnostic Monitor, Visual Space Manager, Database Maintenance Manager, Disaster Recovery Toolset and the White Sands logo are trademarks of White Sands Technology, Inc. Other trademarks are the properties of their respective owners.