****

**Specification**

**for**

**09/20/11**

IderaLogo

Proprietary and Confidential to BBS Technologies, Inc.

**© 2011 BBS Technologies, Inc.; all rights reserved.**

# Revision history:

|  |  |  |
| --- | --- | --- |
| **When?** | **Who?** | **What?** |
| 09/20/2011 | Robert | First Draft |

# Table of Contents

1. Revision history: ii

2. Table of Contents iii

3. Requirements 1

3.1. Overview/Purpose 1

3.1.1. Related Customer Requests 1

3.2. Feature/Function Market Requirements 1

3.2.1. Required Functions 1

3.2.2. Non-Supported Functions 1

3.3. Open Questions 1

4. Functional Design 2

4.1. User Interfaces 2

4.2. Installation and Upgrade 5

4.3. Permissions and other Required Configuration 5

4.4. Licensing Issues 5

4.5. Dependencies 6

4.5.1. Dependencies on Idera Software 6

4.5.2. Third-Party Software Required on the Customer Machine 6

4.5.3. Third-Party Software Required Internally 6

5. Internal Design 6

5.1. Architecture 6

5.2. Installation Issues 7

5.3. Schedule 7

5.3.1. Work Breakdown and Sizings 7

5.3.2. Areas of Risk 7

6. Quality Assurance Considerations 8

6.1.1. Overview 8

7. Documentation Considerations 8

8. Bibliography 8

# Requirements

## Overview/Purpose

Customers need the ability to monitor sensitive columns, when they are accessed and by whom. This feature will add the ability for users to specify certain columns in a table that are sensitive.

### Related Customer Requests

11065 – FRQ: Enhance column level auditability for “select” statements

## Feature/Function Market Requirements

### Required Functions

This feature will allow users to know one or more columns from a table are accessed via a select statement. The workflow is very simple. There will be a Sensitive columns tab on the Audited Database Properties dialog. The user will select which tables and columns for those table that they care to audit.

This feature will not require select auditing to be enabled. A separate trace will be created for Sensitive columns trace for only the table/columns selected.

The user will view the data in the Audit Events view. The data will be formatted similarly to BAD. It will have + next to each select that has sensitive column information available.

There will also be a report that is similar to the Before-After Data report.

### Non-Supported Functions

None

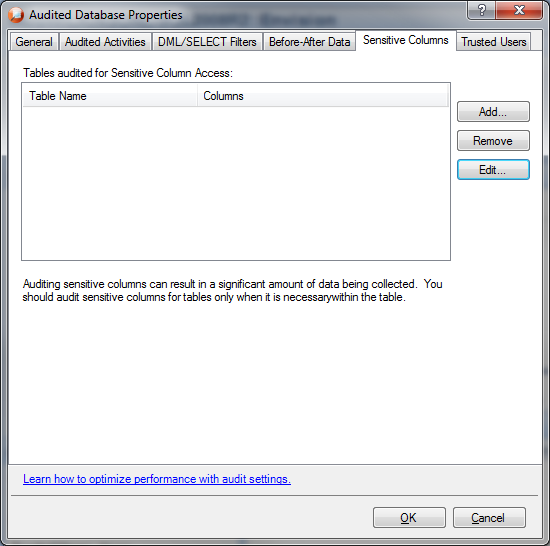
## Open Questions

None

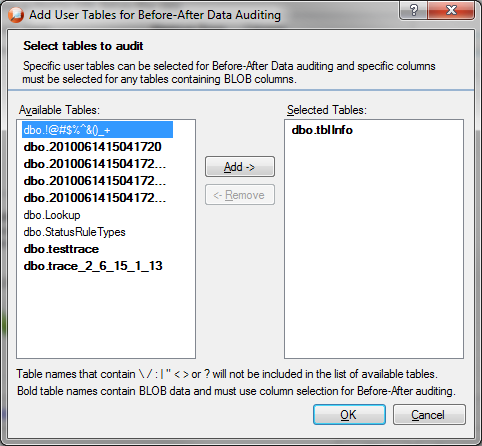
# Functional Design

## User Interfaces

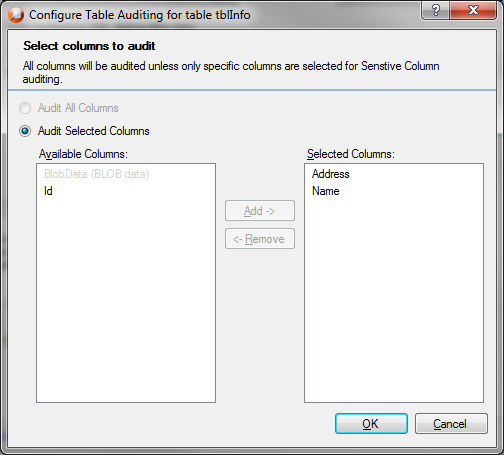
The user will select the tables/columns on the Audited Database Properties dialog.



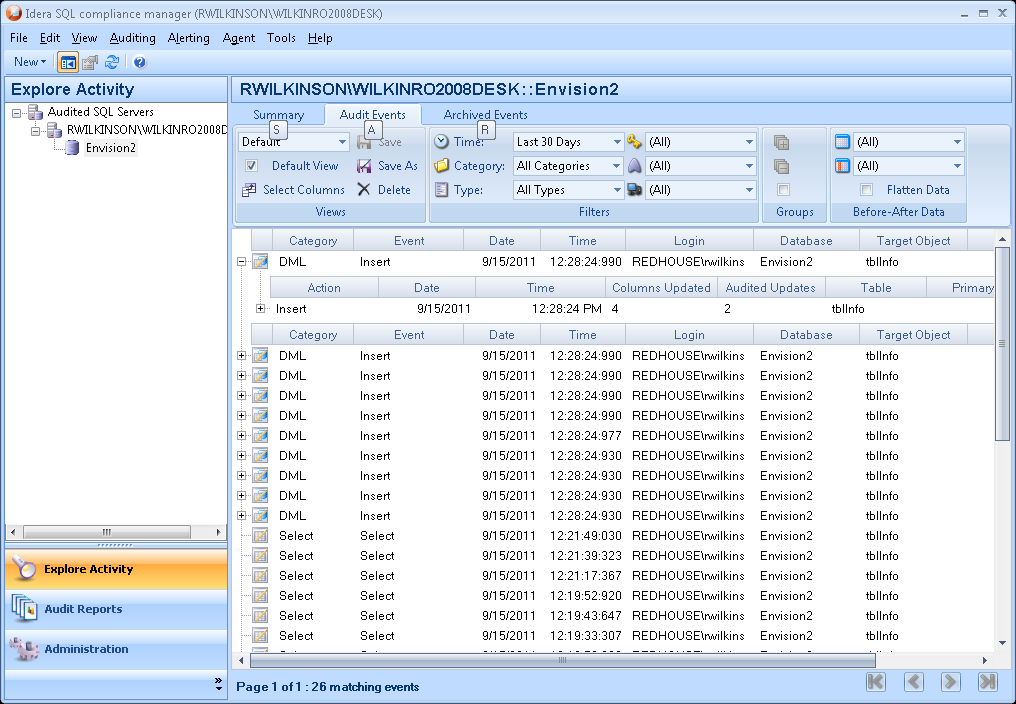
This is what the table selection dialog will look like but will have all the restrictions removed. All tables will be available for Sensitive Column auditing.



Unlike BAD, Sensitive Columns table selection will allow the user to select any column on any table. Blob columns are not an issue for this feature.



The display of the Sensitive Column events will be similar to BAD. The select event will be listed and if the select was obtained from a Sensitive column trace, a + will be placed next to the column. The expanded row will show the event details.



## Installation and Upgrade

None

## Permissions and other Required Configuration

None

## Licensing Issues

None

## Dependencies

None

### Dependencies on Idera Software

None

### Third-Party Software Required on the Customer Machine

None

### Third-Party Software Required Internally

None

# Internal Design

## Architecture

An overview of the architecture behind this feature – how it works, components, communication between components etc

* Desktop Client -
  + Create the new tab and implement the table and column selection dialogs.
  + Change the Event view to display the knew sensitive column data. This will require two new Infragistics bands. One for the select details and one for the list of columns.
  + Create a new report based on the BAD report
* Collection Server –
  + Trace Creation
    - If you database is being audited for both select auditing and sensitive column auditing, combine that into one trace.
  + Trace processing
    - When we get a select event, if we have the SQL text, parse the SQL text but only if that object (table) is being audited for Sensitive column access.
    - The collection server will use the Microsoft TSQL parser.
* Repository Changes -
  + In the SQLcompliance database, Add a Usage column to the DataChangeTables and DataChangeColumns tables. This column will be an int that is a bit mask that tell the console where the column is used, BAD, Sensitive columns or both.
  + In the event database a new table will the added for the accessed columns. This will be similar to the datachanges table. It will have Starttime, eventSeq, spid, column name, eventId, Hashcode, columnId. There will be one row for every column.

## Installation Issues

None.

## Schedule

### Work Breakdown and Sizings

|  |  |  |
| --- | --- | --- |
| Component | Who | Sizing (Days) |
| Desktop Client - properties dialog changes | Robert | 1 |
| Desktop Client – Event view changes | Robert | 2 |
| Desktop Client - New Report | Robert | 1 |
| Collection Server | Robert | 7 |
| Repository Changes | Robert | 1 |
| Testing | Robert | 1 |
| **Total** |  | **13** |

### Areas of Risk

None

# Quality Assurance Considerations

### Overview

The same two tables for configuration will be shared between BAD and Sensitive Columns. When adding a table/column to one, we need to make sure that it doesn’t get added to the other.

# Documentation Considerations

None

# Bibliography