DSAuditor 4.5 User Guide

Embarcadero Technologies, Inc.
100 California Street, 12th Floor
San Francisco, CA 94111 U.S.A.

Contents

Welcome to DSAuditor

DSAuditor helps to secure critical data, ensure data privacy, and enable regulatory compliance by monitoring database access and activity. DSAuditor's ability to detect suspicious behavior in real time minimizes the threat of data theft and tampering. Historical data auditing capabilities deliver detailed reports to comply with stringent internal policies and external regulatory requirements. And, DSAuditor's network-based approach enables reporting on sensitive events such as database, schema, and permissions updates, without impacting performance.

DSAuditor tracks:

- Which tables and columns are being used (and, conversely, which are not)
- Who is accessing the data
- When they are accessing it
- What kinds of activities are occurring

DSAuditor works by “listening” to every SQL query or database request submitted by end user and applications, excluding any that you are not interested in tracking. The queries are then parsed and detailed information written to a repository. A nightly summarization process on the repository consolidate this data into pre-joined, denormalized summary tables.

A browser-based client provides a graphical front-end to both the detail and summary tables to generate customized reports, which can display activity down to the table, column, or individual query level, providing both response time and the number of rows and bytes returned per query.

This document covers only the browser-based client. Information on the installation and operation of the server, data-acquisition, and administrative components of DSAuditor may be found in the *DSAuditor Installation Guide and Technical Reference*. Details of the repository schema can also be found in that document.

Additional Product Resources

The Embarcadero Web site is an excellent source for additional product information, including white papers, articles, FAQs, discussion groups, and the Embarcadero Knowledge Base.

Go to www.embarcadero.com/support, or click any of the links below, to find:

- Documentation
- Online Demos
- Technical Papers
- Discussion Forums
- Knowledge Base

Embarcadero Technologies Technical Support

If you have a valid maintenance contract with Embarcadero Technologies, the Embarcadero Technical Support team is available to assist you with any problems you have with our applications. Our maintenance contract also entitles registered users of Embarcadero Technologies’ products to download free software upgrades during the active contract period.

To save you time, Embarcadero Technologies maintains a Knowledge Base of commonly-encountered issues and hosts Discussion Forums that allow users to discuss their experiences using our products and any quirks they may have discovered.

To speak directly with Embarcadero Technical Support, see Contacting Embarcadero Technologies Technical Support below.

NOTE: Evaluators receive free technical support for the term of their evaluation (14 days).

Contacting Embarcadero Technologies Technical Support

When contacting Embarcadero Technologies Technical Support please provide the following to ensure swift and accurate service:

Personal Information

- Name
- Company name and address
- Telephone number
- Fax number
- Email address

Product and System Information

- Embarcadero product name and version number. This information is found under Help, About.
- Your client operation system and version number.
- Your database and version number.

Problem Description

A succinct but complete description of the problem is required. If you are contacting us by telephone, please have the above information, including any error messages, available so that an Embarcadero Technical Support Engineer can reproduce the error and clearly understand the problem.

There are three ways to contact Embarcadero's Technical Support department:

- Via the Web
- Via Phone
- Via Email

Via the Web

Embarcadero Technical Support provides an online form that lets you open a Support case via the Web. To access this form, go to http://www.embarcadero.com/support/open_case.jsp.

We normally acknowledge the receipt of every case on the same day, depending on the time of submission.

Via Phone

United States

Embarcadero Technologies Technical Support phone number is (415) 834-3131 option 2 and then follow the prompts. The hours are Monday through Friday, 6:00 A.M. to 6:00 P.M. Pacific time.

For licensing issues, including Product Unlock Codes, call (415) 834-3131 option 2 and then follow the prompts. The hours are Monday through Friday, 6:00 A.M. to 6:00 P.M. Pacific time.

The Embarcadero Technologies Technical Support fax number is (415) 495-4418.

EMEA

Embarcadero Technologies Technical Support phone number is +44 (0)1628 684 499. The hours are Monday to Friday, 9 A.M. to 5:30 P.M. U.K. time.

For licensing issues, including Product Unlock Codes, call +44 (0)1628-684 494. The hours are Monday to Friday, 9 A.M. to 5:30 P.M. U.K. time

The Embarcadero Technologies Technical Support fax number is +44 (0)1628 684 401.

Via Email

United States

Depending on your needs, send your email to one of the following:

- support@embarcadero.com - Get technical support for users and evaluators
- upgrade@embarcadero.com - Request upgrade information
- key@embarcadero.com - Request a product key
- wish@embarcadero.com - Make a suggestion about one of our products

EMEA

Depending on your needs, send your email to one of the following:

- uk.support@embarcadero.com- Get technical support for users and evaluators
- uk.upgrade@embarcadero.com - Request upgrade information
- uk.key@embarcadero.com - Request a product key
- uk.wish@embarcadero.com - Make a suggestion about one of our products

Dashboard Charts

View Charts

DSAuditor includes 29 “dashboard” charts for commonly required performance-, privacy-, and security-related auditing tasks.

> **NOTE:** Several shared filters must be modified before these charts will be accurate and useful. For details, see Modify Default FIlters Used by Charts.

To view a chart, hover the mouse pointer over **Security**, **Privacy**, or **Performance** in the top menu, then select a category from the submenu:

Top Menu	Submenu	Chart (click for description)
Performance	Column Usage	Top 25 Column Accesses, Top 25 Column Updates
	Dormant Objects	Dormant Columns, Dormant Tables
	Long Running	Top 25 Largest Data Returns, Top 25 Longest Running Queries
	Table Joins	Table Join Summary - Month-to-Date, Table Join Summary - Last Year, Month-to-Date
	Table Usage	Table Accesses, Table Updates
Privacy	Non-Privileged Users	Failed Selects by Non-Privileged Users, Large Selects by Non-Privileged Users, Non-Privileged Select Activity Total, Non-Privileged Select by Table, Select Activity by Non-Privileged Users
	Privileged Users	Failed Selects by Privileged Users, Large Selects by Privileged Users, Select Activity by Privileged Users
Security	Data Changes	Data Changes by Privileged Users, Data Changes by Unauthorized Applications
	Logins	Login Source Information, Non-Privileged Normal Business Hour Logins, Non-Privileged Off-Hour Logins, Privileged Normal Business Hour Logins, Privileged Off-Hour Logins
	Permissions	Grant-Revoke Activity, Role and User Account Activity
	Schema Changes	Database Schema Change Summary, Schema Changes by Unauthorized Applications

The **Refreshed** field at the top of the report indicates the last time the report was updated. To update again, click the **Refresh** icon in the upper-right corner. If the chart is blank, there may be no data within the selected date range.

To see the SQL query that generates the chart, click the **sql** icon in the upper-right corner.

Modify a Chart

To change the date range of a chart, change from chart to table view or vice-versa, or select a different chart type, click the **Configure** (wrench) icon in the upper-right corner of the chart.

NOTE: If you set the date range so as to return an enormous amount of data, for example by selecting **All Dates Through Today**, after you save the configuration it may take several minutes for the chart to be updated. If the results are too dense to be readable, try switching to table view.

Chart Descriptions

Performance Charts - Column Usage

Column usage is important to continuously monitor in order to understand historical trends for data warehousing optimization as well as security.

Top 25 Column Accesses: This chart provides information on the top 25 columns accessed (select activity) for the monitored databases for the last 7 days.

Top 25 Column Updates: The Column Updates chart shows the top 25 updated columns per database instance for the last 7 days.

Performance Charts - Dormant Objects

Dormant Table charts are used to streamline the data being loaded into the DSS database. For example, data accessed only once per month can be loaded on a different schedule than data accessed on a daily basis.

Unused Table charts are used to aide in re-design of the DSS database eliminating unutilized Tables and improving the ETL process performance.

Dormant Columns: The Unused Columns chart shows columns that have not been accessed in the last 90 days. This data may no longer be required by the application or may be redundant.

In addition, these columns may contain sensitive data and should be evaluated for business risk.

Dormant Tables: The Unused Tables chart shows tables that exist in the database that have not been accessed in the last 90 days. This data may no longer be required by the application or may be redundant.

In addition, these tables may contain sensitive data and should be evaluated for business risk.

Performance Charts - Long Running

Long running queries are often indicative of SQL that needs to be tuned, missing indexes, or the need for summarized data. The Longest Running Query chart is used to target a set of queries to optimize. The overall query performance on the database is improved as well because optimizing long running queries frees up database resources for other queries. The Longest Running Query chart is used to identify users who require more understanding of data farming. Identifying and training power users can have a significant impact on system performance.

Top 25 Largest Data Returns: Queries returning a large amount of data can affect performance. Use a detailed report to analyze these queries and determine if they can be optimized.

Top 25 Longest Running Queries: Long running queries affect application performance. By analyzing the full SQL statements in a detailed report you may be able to better optimize the queries for improved transaction times.

Performance Charts - Table Joins

If tables were joined less in the past month than in the same period of the previous year, that may indicate that their indexes can be deleted. An increased number of joins may indicate the need to optimize the join order or create an aggregation table to improve performance.

Table Join Summary - Month-to-Date: Shows usage for each table that was joined in a query.

Table Join Summary - Last Year, Month-to-Date: Shows usage for each table that was joined in a query.

Performance Charts - Table Usage

Table usage is important to continuously monitor in order to understand historical trends for data warehousing optimization as well as security. Table usage charts are used to assess the proper usage of the DSS data. The Table usage charts will identify the most heavily used tables. This information can then be used to reorganize the ETL process to insure that the most important table are loaded first.

Table Accesses: Shows usage for each table that was used in a Select query.

Table Updates: Shows usage for each table that was used in a Delete, Insert, or Update query.

Privacy Charts - Non-Privileged Users

One of the major components of data privacy is having a record of who simply viewed Personally Identifiable Information (PII) or Protected Health Information (PHI). This requires the monitoring of SELECT statements, and ensures that companies can respond to customer's inquiries about who has seen their information.

Unusual variations in activity could indicate unauthorized viewing or downloading of data to a local system and detailed audit trails will enable companies to accurately determine the extent of a breach, limiting the losses. While you would expect application users to frequently access a small number of records, generally it would be unusual for them to SELECT most or all of the database records. All SELECT activity that does not come from an authorized application should be investigated.

References

Non-privileged User Data Access: PCI-DSS 10.2.1, HIPAA 164.308(a)(1)(ii)(D), CMS-ARS 11.6, GLBA §314.3(b)(3), Basel II/ISO 17799 §10.10.1

Failed Selects by Non-Privileged Users: Through the normal course of business various things can happen to cause a command to fail. A consistently large volume in comparison to overall activity could indicate problems with your application(s) or users attempting to access the data outside of the approved applications. An unusual spike in activity; however, likely indicates that someone is “probing” the database for access points.

Large Selects by Non-Privileged Users: Every organization will have a different definition of “large” and some databases will have a wider variation in their activity. However, once you have monitored SELECT activity for several weeks it should be relatively clear as to a threshold that represents an unusually large dataset return.

This represents a likely download of the data to a local database or even Excel spreadsheet. Once the data is stored locally, you've likely lost the ability to place controls on that data. Many of today's data breach headlines are of this nature: a lost laptop, CD, or file containing unencrypted sensitive data such as Social Security numbers.

It may also violate privacy regulations such as the HIPAA requirement that only those with the “need to know” can see a patient's Protected Health Information (PHI). For example, a case worker should only see the data on the patients assigned to them, not all patient records stored in the database.

Non-Privileged Select Activity Total: Adjusting for seasonal changes and major changes in the business, total Select activity should remain relatively stable. Unusual trends or spikes should be investigated immediately to determine if a user is downloading data over time rather than all at once.

Non-Privileged Select by Table: It goes without saying that some tables are more important than others. Monitoring total Select activity on these tables will enable you to detect trends in usage. Unexplained increases not caused by business reasons and short-term spikes should be further investigated.

Select Activity by Non-Privileged Users: Generally, non-privileged users should be accessing data through an application interface. They are going to generate a high-volume of SELECT activity because it is part of their job function to interact with the data.

An unusual increase in the amount of activity in this area without a corresponding increase in the number of end-users could indicate users viewing data for unnecessary purposes. Keep in mind though that with certain applications (such as databases supporting financial applications) there are normal seasonal spikes in activity.

A steady, incremental rise in activity likely indicates an increase in the total number of end-users. If your organization isn't growing you may want to investigate this. Start by looking at the Security - Permissions charts to see if more users are being granted access to the database.

Privacy Charts - Privileged Users

One of the major components of data privacy is having a record of who simply viewed Personally Identifiable Information (PII) or Protected Health Information (PHI). This requires the monitoring of SELECT statements, and ensures that companies can respond to customer's inquiries about who has seen their information.

Unusual increases in activity could indicate unauthorized viewing or downloading of data to a local system, where it is much more difficult to protect and monitor. In addition, detailed audit trails will enable companies to accurately determine the extent of a breach, limiting the losses. SELECT activity should be minimal for Privileged Users.

References

Sarbanes-Oxley/CobiT §DS 5.5, PCI-DSS 10.2.2, HIPAA §164.312 (b), CMS-ARS 11.1, FDA 21 CFR Part 11 §11.10(e), GLBA/FFIEC Information Security Handbook p. 16, Basel II/ISO 17799 §10.10.4, FISMA/NIST 800-53 §AU-2, NERC CIP-007-1 §R6.3

Failed Selects by Privileged Users: Through the normal course of business various things can happen to cause a command to fail. Particularly in the case of privileged users, who should not be issuing a large number of SELECT statements, the volume of failed commands should be very low. A consistently large volume in comparison to overall activity could indicate that your privileged users don't actually have the access they need to do their jobs. An unusual spike in activity; however, likely indicates that someone is “probing” the database for tables they can access.

Large Selects by Privileged Users: Every organization will have a different definition of “large” and some databases will have a wider variation in their activity. However, once you have monitored SELECT activity for several weeks it should be relatively clear as to a threshold that represents an unusually large dataset return.

In the case of privileged users this represents a likely download of the data, possibly to use for testing purposes. In the case of sensitive data, communicate with the user to ensure they have a legitimate need for the data and understand the protection requirements for that data. Use of “live” customer names, addresses, and account IDs or Social Security numbers by development and test personnel may be a violation of privacy law or your organization's privacy policy and should be avoided if possible.

Select Activity by Privileged Users: Privileged Users should be administering access to the database, making necessary changes to the structure, and performing other maintenance activity. They should not have much need for direct access to data and thus should issue a very limited number of SELECT statements against production data, especially sensitive data.

An unusual increase in the amount of activity in this area could indicate a Privileged User that is also functioning as an end-user. This is likely a breach of Segregation of Duties requirements and at the very least the user should be performing that activity using an application account, not their privileged database account. This could also be an indication that a Privileged User is “downloading” the data to a local database in small chunks.

A steady, incremental rise in activity likely indicates an increase in the total number of Privileged Users. If your organization isn't growing you may want to investigate this. Start by looking at the “Permissions” charts.

Security Charts - Data Changes

Certain regulations such as Sarbanes-Oxley and FDA 21 CFR Part 11 are focused primarily on data integrity. While data changes are a normal part of business function, it is import to record information about these changes in the event of an unauthorized change. In particular it is important to monitor data changes made by privileged users and changes made outside expected applications as these changes circumvent application controls.

References

Sarbanes-Oxley/CobiT §DS 5.5, PCI-DSS 10.2.2, HIPAA §164.312 (b), CMS-ARS 11.7, FDA 21 CFR Part 11 §11.10(e), GLBA/FFIEC Information Security Handbook p. 64, Basel II/ISO 17799 §10.10.4 §12.2.2 §15.1.4, FISMA/NIST 800-53 §AU-2, NERC CIP-007-1 §R6.3

Data Changes by Privileged Users: Changes to production data should be made via applications, not directly by privileged users. Sensitive production data should be closely monitored for any updates.

Data Changes by Unauthorized Applications: Inserts, Updates, and Deletes made month-to-date by unauthorized applications. Changes to production data should be made only via authorized applications via corporate policy.

Security Charts - Logins

Login activity, both successful and unsuccessful, provides an organization with critical information for monitoring and investigating security events. Other access control requirements include assigning unique user IDs, strong passwords, and a good user account management process.

References

- ·Failed Logon Attempts: Sarbanes-Oxley/CobiT 4 §DS5.5, PCI-DSS §10.2.4, HIPAA §164.308 (a)(5)(ii)(C), CMS-ARS §11.1, FDA 21 CFR Part 11 §11.1, GLBA/FFIEC Information Security Handbook p. 65, Basel II/ISO 17799 §10.10.1, FISMA/NIST 800-53 §AC-6, NERC CIP-007-1 §R6.3
- ·Unique User IDs: Sarbanes-Oxley/CobiT 4 §DS5.3, PCI-DSS §8.1, HIPAA §164.312(a)(2)(i), CMS-ARS §3.12 and 7.7, FDA 21 CFR Part 11 §11.300(a), GLBA/FFIEC Information Security Handbook p. 65, Basel II/ISO 17799 §11.2.1, FISMA/NIST 800-53 §IA-2 and IA-4, NERC CIP-007-1 §R6.3

Login Source Information: This table provides you with metrics to spot likely use of a shared account. User IDs with a significant number of logins in one day or coming from multiple network users, multiple source IP addresses or multiple source applications are highly suspicious and should be investigated. It is also highly unlikely that a single user would log in from multiple domains during a single 24-hour period. Some of this may vary from organization to organization, but by monitoring this information over time you will gain an understanding of what is “normal” for your organization and quickly be able to spot anomalies.

Non-Privileged Normal Business Hour Logins: It is important to monitor both failed and successful logins as part of your arsenal to detect unauthorized access. A significant change in either component, or the ratio between the two, is a likely indicator of a security incident and should be investigated further.

Non-Privileged Off-Hour Logins: A quick comparison from this graph to the “Non-Privileged Normal Hours Logins” will tell you if you are seeing the appropriate drop-off in login activity after hours. If not, run a detailed report and drill down to see if a majority of the off-hours logins are occurring near your cut-off hours - you may need to simply revise the filter to adjust the hours.

Privileged Normal Business Hour Logins: It is important to monitor both failed and successful logins as part of your arsenal to detect unauthorized access. A significant change in either component, or the ratio between the two, is a likely indicator of a security incident and should be investigated further.

Privileged Off-Hour Logins: A quick comparison from this graph to the “Privileged Normal Hours Logins” will tell you if you are seeing the appropriate drop-off in login activity after hours. If not, run a detailed report and drill down to see if a majority of the off-hours logins are occurring near your cut-off hours - you may need to simply revise the filter to adjust the hours.

Security Charts - Permissions

Access Control is fundamental to ensuring both data security and privacy. Monitoring GRANT and REVOKE statements on your databases provides you with a record of permission changes and enables you to identify unusual activity including user-defined roles that may be created without proper authorization. It is generally considered best practice to grant permissions to roles, not directly to users, to provide better controlled permissions management.

References

Sarbanes-Oxley/CobiT §DS 5.5, PCI-DSS 10.2.5, HIPAA §164.312 (b), CMS-ARS 11.1, FDA 21 CFR Part 11 §11.10(e), GLBA/FFIEC Information Security Handbook p. 16, Basel II/ISO 17799 §10.10.1, FISMA/NIST 800-53 §AU-2, NERC CIP-007-1 §R6.3

Grant-Revoke Activity: For a production database, permission changes should be monitored weekly. Grant and revoke activity should map to application user provisioning. It is important to look for unusual database authorizations as it could indicate unauthorized access. For example, a common database threat is role-escalation and may be done during a short time window. Investigate grant-revoke activity to ensure that permission changes were made per an authorized change request. Also if you see an increasing deviation between Grants and Revokes you may have too many users with too many privileges, a problem that only gets worse with time. Review your de-provisioning process to ensure proper notification when users/roles no longer need all the permissions granted to them.

Role and User Account Activity: Per database security best practices, roles and user accounts are instrumental for ensuring sound security.

Roles should be used when provisioning new database user accounts. Database roles should be fairly static for production databases and therefore, should track with application changes and upgrades. Create Role, Alter Role, and Drop Role metrics should be monitored regularly.

Database account activity should be monitored including provisioning and deprovisioning users. When OS accounts are deprovisioned, the matching database accounts should be removed as well. If your organization is not growing, but you see many more roles and users created than dropped, you should review your de-provisioning process.

Security Charts - Schema Changes

Unauthorized and undetected changes to a database schema can cause system instability at the very least or result in theft of assets in a worst-case scenario. Procedures should be in place to ensure that changes made to the database schema are done in a controlled and authorized fashion and all schema changes should be monitored on critical databases. A help desk system should be used to issue, track, and record changes for every production database.

References

Sarbanes-Oxley/CobiT §DS 5.5, PCI DSS §10.2.7, HIPAA §164.312 (b), FDA 21 CFR Part §11 11.10(e), GLBA/FFIEC Information Security Handbook p. 64, Basel II/ISO 17799 §10.10.1, FISMA/NIST 800-53 §AU-2, NERC CIP-007-1 §R6.3

Database Schema Change Summary: Database schema change activity should be monitored and audited weekly or monthly to ensure that the change management process is being followed.

Normally spikes in activity are considered an indicator of risk. However, if your organization has a well-controlled change management process, this could be a normal pattern of activity bundling a number of database schema changes together and would map to a Systems Development Lifecycle of Develop, Test, Release.

Ensure that spikes in activity correspond to authorized changes in the database and spot-check lower levels of changes between these releases to ensure that they are also following change management processes. Frequent, small number of changes may indicate a lot of unmanaged “tweaking” of the database that increases your risk of outages, and should be investigated to ensure it makes sense from a business and security perspective.

Schema Changes by Unauthorized Applications: In a well-controlled environment, database schema changes should be made only by authorized applications that include good access and auditing controls. Any instance of a change made by an unrecognized application should be investigated to ensure that your change control processes have not been circumvented and that a change has not been made by an unauthorized user.

Reports

Understanding Reports

For auditing requirements not met by the dashboard charts, you may create reports. These reports may include more detailed data, and allow you to “drill down” from summary to detailed data, in some cases all the way down to the individual query level. You may “publish” a report to share it with all other users, annotate reports with comments that are visible to other users, and save reports in HTML, PDF, comma-delimited text, or rich text formats.

Reports have the following band-oriented structure:

Report title	
Report description	
One or more subreports, each including:	Subreport title
	Optional header showing date range, grouping, sort, content, and filter settings
	Body
	Optional signature section (included only when exporting to PDF or RTF)

The subreport body content is defined by setting the following subreport properties in a report template:

- **Type**: A subreport’s basic qualities are defined by selecting one of following nine types:

  Column Summary, **Query Summary**, **Table Summary**, and **Table Join Summary** subreports provide summary information on column accesses, query counts, table accesses, and join activity, respectively.

  Dormant Column and **Dormant Table** subreports provide information on columns and tables which have not been accessed in a certain amount of time. Dormant data is defined as a column or table which was used at one time but has not been accessed in a certain number of days. Unused data is defined as a column or table which has never been used. Both types of data can be shown on the same report.

  NOTE: For the above summary and dormant subreports to be accurate, the STIReader, STIWriter, and DBSummarizer server components must be configured and operating correctly. The following reports do not depend on those server components.

  Query Detail subreports can be used to show individual queries that meet specified selection criteria such as the number of rows returned or execution time. Rejected queries can also be shown using this report.

  Repetitive Query subreports show queries that have been duplicated more that a certain number of times.

  Session Detail subreports shows one row of detail for each logical connection to the DBMS. Failed login attempts can be displayed with this report.

  NOTE: The Query Detail [verify], Repetitive Query, and Session Detail subreports can be configured to show the full query text, the first line of the text, or no query text.

- **Include Header Page / Include Signature Page**: enables / disables optional header and signature
- **Date Range**: The range of dates to be included in the report. **Preset** date ranges are relative to the day the report is run. **Custom** date ranges are static. For more information on preset date ranges, see Subreport Attribute Value Descriptions

- **Content**: Selects which fields will be included in each row of the subreport body. Which fields are available depends on the **Type** setting. For more information on these fields, see Subreport Attribute Value Descriptions.
- **Sort Order**: Controls how the rows in the subreport body are sorted. Which sort options are available depends on the **Type** setting. For more information on these options, see Subreport Attribute Value Descriptions.
- **Row Limit**: If **All Rows** is selected, the report will include all data. If **Top** is selected and a top value of *n* specified, the subreport's tables will include only the first *n* rows of the sorted results. For example, if in a Query Detail subreport you set the **Top** value to 5, and the sort order was Rows Affected / Descending, the subreport would include the five queries that affected the most rows during the selected date range.
- **Grouping**: The criteria by which the rows in the report are to be grouped. Which grouping criteria are available depends on the **Type** setting.

  You may specify up to five nested levels of grouping criteria, for example by table name broken down by day of the week. Summary and dormant report types must have at least one grouping level.

  Optionally, each group may include totals and/or a summary chart.

  For more information on these criteria, see Subreport Attribute Value Descriptions.
- **Filter**: Allows you to narrow the query used to create the subreport body. For example, you could limit a Table Summary report to include only SELECT query data. For instructions on defining filter criteria, see Create or Edit a Shared Filter.

Create and Publish a New Report

1. Select **Reports > Templates**.
2. Click the name of the template from which you want to create the report. (If no appropriate template exists, see Create or Edit a Report Template).
3. Click **Create Report**.
4. Use the **Table of Contents** to navigate through the report and "drill down."

   To view detailed metadata and statistics for an individual query, plus (if allowed by the DSAuditor server administrator) its SQL query text, click the contents of the first field of its row (typically the client application name). This will permanently add a Query Instance report to the subreport's appendix.

   To export to a file, under **Export** click **HTML**, **PDF**, **CSV** or **RTF**. Any existing Query Instance reports are included in the export; detailed data for other queries is not.
5. To make this report available for viewing by other users, click **Publish** to add it to the **Reports** list. (By default, this command is available only when logged in with Power User or Administrator privileges; for more information, see Understanding Role-Based Security.)

View or Export a Published Report

NOTE: The Reports list is empty until someone creates a report from a template and publishes it. For more information, see Create and Publish a New Report.

1. Select **Reports**.
2. Click the name of the report. If it includes a lot of data, it may take a few minutes to display.

3 Use the **Table of Contents** to navigate through the report and “drill down.”

To view detailed metadata and statistics for an individual query, plus (if allowed by the DSAuditor server administrator) its SQL query text, click the contents of the first field of its row (typically the client application name).

To update the report with the most recent data, under **Actions** click **Refresh**.

To view the SQL query that generated the report, under **Actions** click **Show SQL**.

To export to a file, under **Export** click **HTML**, **PDF**, **CSV** or **RTF**.

Schedule a Report

The Schedule tool allows you to configure report templates to generate selected reports on defined schedules, such as daily, every Monday, or the first day of every month.

1 Select **Reports > Schedule**. (By default, this command is available only when logged in with Power User or Administrator privileges; for more information, see Understanding Role-Based Security.)

2 Click **New Schedule**.

3 Select the template for the report to be scheduled.

4 Optionally, set a date range to override the template’s date range.

5 Set the recurrence options, then click **Save**.

Reports will now be generated from the selected template as specified by the recurrence options. Once generated, the reports can be viewed by clicking the links in the Report Calendar or on the Reports page.

Modify a Report

You can modify a report only by adding comments and by “drilling down” (which adds Query Instance reports to the subreport’s appendix).

To make other changes, modify the template the report is based on, or create a new variation of that template, and then create and publish a report. See Create or Edit a Report Template.

Create or Edit a Report Template

NOTE: Changes to a template do not affect previously published reports.

To create a new template based on an existing one:

1 Select **Reports > Templates**.

2 Click the name of the template on which the new template will be based.

3 Under Operations, click **Edit New Copy**.

4 Enter a descriptive name for the template.

5 Optionally, modify the description and/or reorder the subreports, then slick **Save**.

6 If you wish to modify a subreport, click its name; under **Operations**, click **Edit**; set the subreport options as appropriate (for more information, see Understanding Reports); then click **Save**. (By default, the **Edit** command is available only when logged in with Power User or Administrator privileges; for more information, see Understanding Role-Based Security.)

7 If you wish to delete a subreport, click its name; under **Operations**, click **Delete**; and click **OK** to confirm.

8 When finished modifying subreports, click **Create Report** to test the template.

To create a template from scratch:

1 Select **Reports > Templates**.

2 Under **Operations**, click **New Template**.

3 Enter a descriptive name and an appropriate description for the template, then slick **Save**.

4 Click **New Subreport Template**.

5 Set the subreport options as appropriate (for more information, see Understanding Reports), then click **Save**.

6 Optionally, add additional subreports.

7 Click **Create Report** to test the template.

Import or Export a Usage Tracker Template

You may share templates with the Windows-based Usage Tracker client using the UTT Import and UTT Export commands.

NOTE: The Chart Style, Include Total, and Include Chart attributes are not included in UTT files, so you must recreate these manually after import.

To import a Usage Tracker template:

1 Select **Reports > Templates**.

2 Under **Operations**, click **Import UTT**.

3 Click **Browse**, navigate to the .utt file exported from Usage Tracker, and double-click it.

4 Optionally, enter a name for the imported template. If you leave the **Template name** field blank, the new template will have the same name as the imported file, minus the .utt extension.

5 Click **Import > Done**.

To export a Usage Tracker template:

1 Select **Reports > Templates**.

2 Click the name of the template on which the new template will be based.

3 Under **Operations**, click **Export to UTT**.

4 *In Firefox*, if prompted, select **Save to Disk**, then click **OK**.

In Internet Explorer, click **Save**.

5 Optionally, select a different directory and/or change the file name, then click **Save**.

Filters

Create or Edit a Shared Filter

If the same filter will be used multiple subreports, you may define it once using the Filters tool. You may then modify the filters of all the subreports at once by editing the single predefined filter. The Web client includes many default filters that can easily be adapted to meet your filtering needs.

NOTE: Some of the sample filters must be edited to meet your company's requirements. For example, in its initial state, the only application recognized by the Authorized Applications filter is DBArtisan. For details, see

1 Select **Reports > Filters**.

2 *To create a new filter from scratch*, click **Create Filter**, then provide a descriptive name for the new filter.

To create a new filter based on an existing one, click the name of the filter on which new one will be based, then click **Edit New Copy**. Provide a descriptive name for the new filter and revise the description as necessary.

To edit an existing filter, click its name, then revise the description to reflect your changes.

CAUTION: When you edit an existing filter, you are revising all templates and reports that use it.

3 Check the subreport types in which you want this filter to be available. When you check or uncheck a type, it may take a few seconds for DSAuditor to rebuild the drop-down menu.

4 Add, delete, or revise filter criteria, shared filters, or groups as appropriate.

NOTE: The icons referred to below appear when you hover your mouse over a filter criterion, shared filter, or **All / One / None of the following must be true** drop-down.

Filter criteria are simplified SQL statements of the format <attribute value> <SQL operator> <string or integer>: for example, Select Count >= 100 or Network User LIKE admin%.

To add a criterion, click the **Add New Criteria** (plus symbol) icon.

Only the attribute values common to all selected subreport types will be included in the drop-down menu and available for use in the filter. See Attribute Value - Subreport Type Concordance for a guide to which attribute values are supported by which types.

To choose a string from a drop-down list of corresponding values in the DSAuditor repository, click the **Toggle List** (magnifying glass) icon. For example, if the Database User attribute value is selected, the drop-down will include all the DBMS user names from all audited queries.

Shared filters may be nested. For example, to find failed selects by unauthorized users outside of normal business hours, you could create a filter combining the Failed Select Queries and Off Hours filters (provided someone had previously edited the latter to reflect your company's business hours). To nest a shared filter, click the **Add Filter** icon (funnel with plus symbol).

A new filter contains a single **Group**, which includes an **All / One / None of the following must be true** drop-down to set the filter to pass rows that meet all, any, or none of the group's criteria. If you have specified a single criterion, **All** and **Any** have the same effect.

Groups may be nested. To add another group, click the **Add To New Group** (right-arrow) icon for one of the filter criteria or shared filters you wish to include in the group. Then use the Add New Criteria, Add Filter, Move Up, or Move Down icons to add other criteria or shared filters to the group.

5 When done setting the above options, click **Save** to create or modify the filter. Then test the filter by running or creating a report that uses it.

Modify Default FIlters Used by Charts

Many of the charts use default shared filters. (For details, see Shared Filters Used in Dashboard Charts.) The following three filters must be modified before running the charts that use them:

- **Authorized Applications**: revise to reflect the DBMS clients, reporting tools, and other executables authorized to access the audited databases
- **Normal Business Hours**: revise to reflect the hours during which DBMS activity expected
- **Privileged Users**: revise to reflect DBAs and others with administrative privileges on the audited databases

The following filters will automatically inherit the above changes:

- Data Changes - Privileged Users
- Data Changes - Unauthorized Applications
- Failed Selects - Non-Privileged Users
- Failed Selects - Privileged Users
- Failed Update Queries
- Large Selects - Non-Privileged Users
- Large Selects - Privileged Users
- Large Selects - Privileged Users - not v$ Tables
- Non-Privileged Users
- Non-Privileged Users - Normal Business Hours
- Non-Privileged Users - Off Hours
- Off Hours
- Privileged Users - Normal Business Hours
- Privileged Users - Off Hours
- Schema Changes by Unauthorized Applications
- Select Queries - Non-Privileged Users
- Select Queries - Privileged Users - not v$ Tables
- Unauthorized Applications

Miscellaneous Tasks

Customize the Web Client

CAUTION: If you use the tools discussed in this section to modify the default client configuration, the instructions in the online help and *DSAuditor User Guide* may no longer be accurate. Consequently, we do recommend you not use this feature.

The DSAuditor Web client is based on Liferay Portal, a highly customizable open-source framework based on the JSR-168 portlet specification. For information on using the **Remove** and **Add Portlet to Column** tools to change what appears on each page, or using the **Content and Layout** to modify the menu structure, see LIferay's documentation:

NOTE: Customization applies only to the current user.

DSAuditor includes the following portlets:

Portlet	Notes
Chart	Displays one of the charts included with the Web client. In the default client configuration, all of these reports are already present in the Security, Privacy, and Performance pages. For more information, see Dashboard Charts.
Filters	Defines a filter (SQL query) for use in a report template. For more information, see Create or Edit a Shared Filter.
My Profile	Allows you to edit your contact information and change your password; see Change Your Password.
Report Calendar	Displays the reports that were or are scheduled to run in the current week. You may click the name of a completed report to view it. In the default configuration, this appears on the Home page. For more information, see Schedule a Report.
Report Schedules	Allows you to schedule reports to run at specified times, once-only or recurring, and to modify or delete previously created schedule entries. For more information, see Schedule a Report.
Report Templates	Lists the templates that define reports, and allows you to create new templates, modify existing templates, or create new reports from templates. For more information, see Create or Edit a Report Template.
Reports	Lists published reports. Click a report name to view it. For more information, see View or Export a Published Report or Create and Publish a New Report.
Repository	Allows users with the Administrator role to specify the connection parameters for the DSAuditor repository database from which reports get their data. For other users, provides a static display of the connection information. For more information, see Set or Change the DSAuditor Repository.
Roles	Allows users with the Administrator role to create and modify additional roles. For more information, see Add a User. By default, this portlet is visible only to users with the Administrator role.
Summarization	Displays date and time the DBSummarizer process completed and its current status. For more information, see the *DSAuditor Installation Guide and Technical Reference.*
Users	Allows users with the Administrator role to add and delete users, change their passwords, and modify contact information. For more information, see Add a User. By default, this portlet is visible only to users with the Administrator role.

Change Your Password

1 Select **User Profiles**.

2 Under **My Profile**, click **Change Password**.

3 Enter the old password once and the new password twice, then click **Save**.

Web Client Administration and Security

The commands discussed in this section are available only to users with Administrator privileges.

Understanding Role-Based Security

What you can do with the Web client is determined by which role is assigned to your login. There are three default roles; in broad summary:

- Users can view dashboard charts, create and export reports, create new report templates, and view and comment on published reports
- Power Users can also publish reports and modify report templates created by other users.
- Administrators can do everything, including create and delete user accounts.

Object	Permission	What It Means	Default Roles		
			User	P.U.	Adm.
DSAuditor Repository Connection	View	View repository connection portlet (always on)	•	•	•
	Modify	Edit repository connection			•
Filter	View	View filters portlet (always on)	•	•	•
	Modify	Edit other users' filters		•	•
	Delete	Delete other users' filters		•	•
Report Templates	View	View report templates portlet (always on)	•	•	•
	Modify	Edit other users' templates		•	•
	Delete	Delete other users' templates		•	•
Reports	View	View reports portlet (always on)	•	•	•
	Modify	Edit other users' comments		•	•
	Delete	Delete other users' reports or comments		•	•
	Publish	Publish reports (if off, Schedules / Modify permission is also off)		•	•
Role-Based Security	View	View roles and users portlets			•
	Create / Modify / Delete	Create/edit/delete roles (except own) that contain a subset of own permissions or users (except own) that hold a subset of own permissions			•
	Create / Modify / Delete All	Unrestricted editing of all roles (except own) and users (except own)			•
Schedules	View	View schedules portlet (always on)	•	•	•
	Modify	Edit other users' schedules (on setting is ignored unless Reports / Publish permission is also on)		•	•
	Delete	Delete other users' schedules		•	•

If the default roles are not appropriate for your needs, you may create new ones. See Add a User.

Add a User

1. Log in with a user ID that has Administrator privileges.
2. Select **User Profiles**.
3. Under **Users**, click **Add User**.
4. Enter the Login Name and password and select one or more roles for the user (see Understanding Role-Based Security). Optionally, enter contact information. Then click **Save**.

Change Another User's Password

When users forget their passwords, an administrator can assign a new one.

1. Log in with a user ID that has Administrator privileges.
2. Select **User Profiles**.
3. Under **Users**, click the name of the user whose password you want to change.
4. Click Edit User.
5. Enter the new password in both fields, then click **Save**.

Create a New Role

To create a new role based on an existing one:

1. Log in with a user ID that has Administrator privileges.
2. Select **User Profiles**.
3. Under **Roles**, click the name of the role (e.g. **Power User**) on which the new role will be based.
4. Click **Edit New Copy**.
5. Enter a descriptive name for the role, check the permissions you wish it to have (see Understanding Role-Based Security), and click **Save**.

To create a new role from scratch:

1. Log in with a user ID that has Administrator privileges.
2. Select **User Profiles**.
3. Click **Add Role**.
4. Enter a descriptive name for the role, check the permissions you wish it to have (see Understanding Role-Based Security), and click **Save**.

View or Modify a Role

NOTE: You can view but not modify the standard User, Power User, and Administrator roles, so their Edit Role commands are disabled.

1 Log in with a user ID that has Administrator privileges.

2 Select **User Profiles**.

3 Under **Roles**, click the name of the role you wish to modify.

4 Click **Edit Role**.

5 Edit the name and/or change the permissions and/or users as appropriate (see Understanding Role-Based Security), then click **Save**.

Delete a Role

NOTE: You cannot delete the standard User, Power User, or Administrator roles.

1 Log in with a user ID that has Administrator privileges.

2 Select **User Profiles**.

3 Under **Roles**, click the name of the role you wish to delete.

4 Click **Delete Role**.

5 Click **OK** to confirm deletion.

6 If any users are assigned only this role and no other, you will be prompted to delete those users. If you are sure that's what you want to do, click **OK** to confirm. Otherwise, click **Cancel**.

Set or Change the DSAuditor Repository

The DSAuditor repository database contains the historical data used in reports (see Welcome to DSAuditor).

To set or change the repository connection properties:

1 Log in with a user ID that has Administrator privileges.

2 Click the Configure (wrench) icon in the upper-right corner of the DSAuditor Repository.

3 Adjust the connection parameters for the DSAuditor repository database as appropriate:

- **Host Name**: the network name of the server running the repository database (if IP Address is specified, this may be left blank)
- **Database Type**: select the platform of the DBMS hosting the repository (for a DSAuditor Appliance or Virtual Appliance using its built-in repository, select PostgreSQL)
- **Database/SID**: the database name or Oracle SID
- **IP Address**: the IP address of the server running the repository database (if Host Name is specified, this may be left blank)
- **Port**: the listener port of the DBMS hosting the repository database

- **User**: a valid user ID for the repository database (by default, admin)
- **Password**: the password corresponding to the user ID

4 Click **Test Connection**.

5 If a “Connection Successful” message appears, click **Save**.

NOTE: If the repository settings appear to be correct, but refreshing a chart does not include data you know exists within the selected date range, contact the DSAuditor server administrator.

Start or Stop the Web Client Server

If the server was installed as a service:

- *To start the server*, in the Windows start menu, select **Embarcadero DSAuditor 4.1 Web Client > Start Web Client’s server**.
- *To stop the server*, in the Windows start menu, select **Embarcadero DSAuditor 4.1 Web Client > Stop Web Client’s server**.

If the server was not installed as a service:

- *To start the server*, in the Windows start menu, select **Embarcadero DSAuditor 4.1 Web Client > Start DSAuditor Web Client’s server**. A command window will open and display a series of startup messages.

  If the server starts successfully, after several minutes you will see a message similar to the following:

  ```
  10:21:22,401 INFO  [Server] JBoss (MX MicroKernel) [4.0.4.GA (build:
  CVSTag=JBoss_4_0_4_GA date=200605151000)] Started in 3m:50s:808ms
  ```

  As users log in and perform tasks on the server the command window will display additional status messages.

- *To stop the server*, close the command window. When prompted to End Now or Cancel, click **Cancel** to allow proper shutdown to continue.

Reference

Subreport Attribute Value Descriptions

The following values are among those used to specify content, sort order, and grouping properties. This is not a comprehensive list; self-explanatory properties such as **Today** and **Query Count** are omitted.

> **NOTE:** **Hour**, **Day**, **Month**, and other time-related values refer to the time the activity occurred. **Quarter** always means standard three-month calendar quarters, never fiscal quarters.

- **Application** is the client or other program used to access the database.
- **Command** is the primary SQL command of a query, such as SELECT, INSERT or UPDATE.
- **Database Instance** is the name of the database accessed.
- **Database Location** is an optional name that may be specified by the DSAuditor server administrator to associate database nodes and source nodes with their physical locations.
- **Database Node** is the IP address of the DBMS host.
- **Database Type** is the DBMS platform: DB2, Informix, Oracle, SQLServer, Sybase, or Teradata.
- **Database User** is the DBMS login used to access the database (see *Network User*.)
- **Department** is an optional name that may be specified by the DSAuditor server administrator to associate users with their departments.
- **Dest Table Name** and **Dest Table Owner** are the name and owner of the destination table of a join. **Dest Qualified Table Name** is a concatenation of the owner and table name separated by a period.
- **Network User** is the login used to log onto the network or the operating system of the DBMS host (see *Database User*).
- **Qualified Column Name** and **Qualified Table Name** are concatenations of the DBMS owner name and the column or table name separated by a period.
- **Query Band** identifies the source collector or SQL trap that audited the transaction. This is an optional string that may be specified by the DSAuditor server administrator; if unspecified, the default value is `AdHoc`.
- **Query Status** is one of the following: complete (C), rejected (R), or indeterminate (I).
- **Source Location** is an optional user-specified name specified with the Table Manager utility.
- **Source Node** is the IP address of the client that originated the activity.
- **Source Table Name** and **Source Table Owner** are the name and owner of a source table of a join. **Source Qualified Table Name** is a concatenation of the owner and table name separated by a period.

Attribute Value - Subreport Type Concordance

This table shows which subreport attribute values are available for use in each subreport type.

	Column Summary	Dormant Column	Dormant Table	Query Detail	Query Summary	Repetitive Query	Session Detail	Table Join Summary	Table Summary
Application				•	•	•	•	•	•
Average Bytes					•	•		•	•
Average End Seconds					•	•		•	•
Average First Seconds					•	•		•	•
Average Packets					•	•		•	•
Average Rows					•	•		•	•
Bytes Returned				•					
Column Clause				•					
Column Name	•	•		•					
Command		•	•	•	•	•		•	•
Create Date		•	•						
Database Instance	•	•	•	•	•	•	•	•	•
Database Location	•	•	•	•	•	•	•	•	•
Database Node			•						
Database Node		•							
Database Node	•	•	•	•	•	•	•	•	•
Database Type	•			•	•	•	•	•	•
Database User	•			•	•	•	•		•
Day	•			•	•	•	•	•	•
Day of Week	•	•	•	•	•	•	•	•	•
Days Since Last Access		•	•						
Department	•			•	•	•	•		•
Dest Qualified Table Name								•	
Dest Table Name								•	
Dest Table Owner								•	
First Access Date		•	•						
First Result Seconds				•		•			
Group By Count	•								
Having Count	•								
Hour				•	•	•	•		•
Indirect Ref Count	•								•
Insert Count	•								
Join Count	•								
Last Access Date		•	•						
Max Bytes					•	•		•	•
Max End Seconds					•	•		•	•

	Column Summary	Dormant Column	Dormant Table	Query Detail	Query Summary	Repetitive Query	Session Detail	Table Join Summary	Table Summary
Max First Seconds					•	•		•	•
Max Packets					•	•		•	•
Max Rows					•	•		•	•
Month	•			•	•	•	•	•	•
Network Packets				•					
Network User	•			•	•	•	•		•
Order By Count	•								
Other Count	•								
Parameter Text				•					
Procedure Name				•					
Procedure Type				•					
Qualified Column Name	•	•							
Qualified Table Name		•	•						•
Quarter	•			•	•	•	•	•	•
Query Band				•	•	•	•		•
Query Count				•	•	•		•	•
Query End Seconds				•		•			
Query Event SN				•					
Query Length				•					
Query Return Code				•					
Query SN				•		•			
Query Status				•	•	•			•
Query Text				•		•			
Query Text (First Row)				•		•			
Rows Affected				•		•			
Select Count	•								
Session End Second							•		
Session ID				•		•	•		
Session Return Code							•		
Session SN				•		•	•		
Session Start Time							•		
Session Status							•		
Source Location	•			•	•	•	•		•
Source Node	•			•	•	•	•		•
Source Qualified Table Name								•	
Source Table Name								•	
Source Table Owner								•	
Table Name	•	•	•	•					•

	Column Summary	Dormant Column	Dormant Table	Query Detail	Query Summary	Repetitive Query	Session Detail	Table Join Summary	Table Summary
Table Owner	•	•	•	•					•
Timestamp				•					
Total Bytes					•	•		•	•
Total End Seconds					•	•		•	•
Total First Seconds					•	•		•	•
Total Packets					•	•		•	•
Total Rows					•	•		•	•
Update Count	•								
Week	•			•	•	•	•	•	•
Where Count	•								
Year	•			•	•	•	•	•	•

Shared Filters Used in Dashboard Charts

The following filters are used by dashboard charts. Some of these filters must be modified before the reports that use them will be accurate; for details, see Modify Default FIlters Used by Charts.

Filter	Used by Report(s)
Data Changes - Privileged Users	Data Changes by Privileged Users
Data Changes - Unauthorized Applications	Data Changes by Unauthorized Applications
Dormant Tables / Columns	Dormant Columns
Dormant Tables / Columns	Dormant Tables
Failed Logins	Non-Privileged Normal Business Hour Logins
	Non-Privileged Off Hour Logins
	Privileged Normal Business Hour Logins
	Privileged Off Hour Logins
Failed Selects - Non-Privileged Users	Failed Selects By Non-Privileged Users
Failed Selects - Privileged Users	Failed Selects By Privileged Users
	Failed Selects By Privileged Users
Grant Queries	Grant-Revoke Activity
Insert or Update Count Greater Than One	Top 25 Column Updates
Large Selects - Non-Privileged Users	Large Selects By Non-Privileged Users
Large Selects - Privileged Users - not v$ Tables	Large Selects By Privileged Users
Non-Privileged Users - Normal Business Hours	Non-Privileged Normal Business Hour Logins
Non-Privileged Users - Off Hours	Non-Privileged Off Hour Logins
Privileged Users - Normal Business Hours	Privileged Normal Business Hour Logins
Privileged Users - Off Hours	Privileged Off Hour Logins
Revoke Queries	Grant-Revoke Activity

Filter	Used by Report(s)
Role and User Activity	Role and User Account Activity
Schema Changes	Database Schema Change Summary
Schema Changes by Unauthorized Applications	Schema Changes by Unauthorized Applications
Select Count Greater Than One	Top 25 Column Accesses
Select Queries	Failed Selects By Privileged Users
	Table Accesses
	Table Accesses
Select Queries - Non-Privileged Users	Non-Privileged Select Activity by Table
	Non-Privileged Select Activity Total
	Select Activity By Non-Privileged Users
Select Queries - Privileged Users - not v$ Tables	Select Activity By Privileged Users
Successful Logins	Non-Privileged Normal Business Hour Logins
	Non-Privileged Off Hour Logins
	Privileged Normal Business Hour Logins
	Privileged Off Hour Logins
Update Queries	Table Updates
	Table Updates