

ApexSQL® Audit 2023.x

Release Notes

These release notes provide information about the ApexSQL® Audit 2023.x which is a major release.

Topics:

- About ApexSQL Audit
- New features
- Getting Started
- System requirements
- Product licensing
- Release History
- About us

About ApexSQL Audit

ApexSQL Audit is a SQL Server auditing and compliance tool with a wide range of features for auditing access, changes, and security on SQL Server instances, databases, and objects. It audits queries, DDL and DML operations, security events (authentication changes, permissions changes, and attempted logins), events on stored procedures and functions, and provides out-of-the-box compliance templates such as HIPAA, GDPR, PCI. ApexSQL Audit saves captured information in a centralized auditing repository and provides comprehensive reports.

New Features

This version of ApexSQL Audit introduces the following new features, enhancements or deprecations:

Enhancements:

- Additional logging is available by activating Debug mode.
- Additional processing of files from the ActiveSessions folder after encountering 3rd party

- parsing errors
- Creation of zipped files containing details about the queries which could not be processed
- Optimization of the Before-after trigger installation process for databases with a large number of Primary Key indexes.
- Support for hosting the Central Repository and auditing events for SQL Server 2022.

Fixes:

- 219140: API JSON output adds comma characters at the end when 'eventsPerPage' value from the URL is greater than 50,000.
- 220351: API call link cannot be opened in the browser (or used to generate data in power BI) when logged in as a user different to the one running ApexSQL Audit central.
- 221921: DML operations inside of a stored procedure are not audited when using Extended event data collection.
- 222518: The auditing configuration is not applied due to timeout being strictly defined as a 10-second value that is now set to follow global timeout settings.
- 222602: Application log messages are incorrectly labelled as INFO instead of ERROR when an error occurs while creating audit sessions.
- 222847: Package is not quarantined when a SQL Query operation type is not extracted correctly from query text data in a specific case.
- 223536: Cannot parse "Deny a permission to principal" operation when there are blank spaces at the end.
- 224205: An Extended event session file containing auditing data gets deleted by SQL Server when a very large number of operations is being executed
- 221223: 'Saving configuration was not successful' message is displayed when trying to exclude a local login in a domain environment
- 225537: SQL Audit auditing configuration is only partially applied when a database which doesn't exist anymore is included in the configuration filters
- 225485: Auditing configuration is only partially applied when there is an ApexSQL Audit Extended event session on SQL Server in stopped state
- 227648: 'Saving configuration was not successful' error is encountered when applying a Before-after configuration for an Availability Group
- 227647: 'Error connecting to server' is encountered when trying to add a database after an Availability group has been added for auditing
- 227557: Error 'Msg 10314, Level 16, State 11' is encountered when trying to update a table on the (new) primary AG replica after a failover
- 227466: SQL Audit database session is not properly created after a failover occurs in an Availability Group
- 228349: An Availability Group cannot be added via listener name if the FQDN of the listener is used
- 227237: AG cluster cannot be added via listener name if the name doesn't match the one given to the Availability Group
- 228615: Incomplete data after reading Microsoft Extended Event file using the MS function - fn_xe_file_target_read_file
- 228776: Auditing sessions are not properly created when a specific combination of filters is used

- 228590: The Before-after section of the UI is not responsive when adding a database with a large number of Primary Key indexes.
- 219710: 'Saving configuration was not successful' is displayed when trying to apply a Before-after configuration with a large number of tables and columns
- 229130: Tables are not successfully loaded in the Before-after configuration when adding a database with specific case-sensitive collation settings
- 229547: 'MERGE INTO' operation is captured as 4 events when using SQL Audit data collection
- 229583: 'DBCC CHECKDB' command is captured with a duplicate record when using SQL Audit data collection
- 229666: Continuous connection timeouts occur because the max pool size has been reached
- 229601: Extended event and SQL Audit sessions are improperly filtered on the SQL instance for all databases except the first one from ApexSQL Audit's configuration filters
- 229777: Auditing agent processes for Always On and FCI clusters are not successfully updated after an upgrade to a new version
- 229779: SQL Audit and Extended event sessions are not properly created when system databases are added for auditing

Changes:

- The column order of Before-after reports has been modified and is now displayed in alphabetical order. This modification enables a significant performance improvement both during the initial setup and when updating the configuration for Before-after auditing

Getting Started

- For further information about installation and getting started, please check the [Quest Knowledge Base](#) or [ApexSQL Getting Started](#).

System requirements

Before installing or upgrading Short Product Name Version, ensure that your system meets the following minimum hardware and software requirements.

Hardware

Dual Core 2.0 GHz CPU

4GB memory

125 MB disk space ^[6]

Port

TCP port 64561 and 60408 on all SQL Server instances (configurable)

Built-in reporting API:

TCP port 49152 on central ApexSQL Audit instance (configurable)

SQL Server

SQL Server 2005 and higher ^[1]

OS

Windows 7 SP1/Windows Server 2008 R2 SP1 and higher ^[1]

Software

[.NET Framework 4.7.2](#) or higher

SQL Server 2008 or higher ^[1], for the Central repository database

Note

SQL Server Express edition is not recommended for the Central repository database, due to the database size limitation

Permissions and additional requirements

Windows user account with administrative privileges

Central repository database must be located on the central ApexSQL Audit instance

See [ApexSQL Audit - Permissions and requirements](#)

Built-in reporting API:

Windows user account with [ApexSQL Audit access](#)

Trusted SSL certificate

See: [Using API to generate SQL auditing reports](#)

Product licensing

ApexSQL offers 2 types of licenses:

1. Individual license

For applications licensed per user, an individual license is for the use of a single user only. This means that only 1 user can use 1 license. If there are multiple users, multiple licenses are needed.

For applications licensed per instance, an individual license is to be used on a single SQL Server instance only. If there are multiple instances, multiple licenses are needed.

2. Enterprise license

An enterprise license can be activated on an unlimited number of instances and can be used by an unlimited number of users, without geographical limitations.

Release History (release notes)

Release: 2023.01.2238

Date: January 17, 2025

Fixes:

- 235808: 'Auditing filter change monitor' alert information is not displayed in full due to character limitation for the [UserSummary] column in [ApexSQL].[AlertReports] table

Release: 2023.01.2237

Date: October 21, 2024

Fixes:

- 217144: Any windows administrator can access ApexSQL Audit UI by default

Release: 2023.01.2231

Date: February 20, 2024

Fixes:

- 229929: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains multiple inserts and an 'EXEC sp_execute' procedure
- 230015: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains a remote procedure call
- 229938: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains 'CREATE SECURITY POLICY' statement
- 230917: Extended event sessions are created with an incorrect file extension when a server is added for auditing using its FQDN
- 230762: The Distributed process is continuously restarted with a 'MaxDegreeOfParallelism' exception when adding a server with 64 cores for auditing

Release: 2023.01.2228

Date: January 23, 2024

Fixes:

- 229880: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains 'EXECUTE AS LOGIN' statement
- 229881: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains a 'value()' method inside of a WITH clause
- 229924: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains 'FOR JSON' clause
- 229925: SQL Parser throws a syntax error during the parsing of a T-SQL query that

- contains the keyword 'next' in conjunction with an object named 'next'
- 229926: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains 'SELECT TOP N.TABLE_NAME.COLUMN_NAME' query which is inside of an INSERT statement
 - 229927: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains a 'UPDLOCK' table hint followed by the 'AS' keyword for the table alias
 - 229928: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains 'OPTION (QUERYTRACEON 9481)' clause
 - 229939: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains 'ALTER SECURITY POLICY' statement
 - 229940: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains 'REVOKE SELECT ON' statement
 - 229973: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains DROP SECURITY POLICY IF EXISTS' statement
 - 230086: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains an execute procedure statement with a number parameter after the semicolon
 - 230311: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains a 'MERGE INTO' statement with 'WHEN NOT MATCHED THEN INSERT DEFAULT VALUES'
 - 230479: SQL Parser throws a syntax error during the parsing of a T-SQL query when an 'UPDATE()' function is executed inside of a CREATE TRIGGER or UPDATE TRIGGER Statement

Release: 2023.01.2224

Date: September 26, 2023

Fixes:

- 230016: ApexSQL Audit is not able to create separate processes for multiple Availability Groups hosted on the same SQL instance
- 225796: The folder MSSQLSERVER is created for an Availability Group replica's temporary files regardless of whether they are named or default instances
- 230120: SQL Parser throws a syntax error during the parsing of an internal query of the DBCC CHECKDB command
- 229931: SQL Parser throws a syntax error during the parsing of a T-SQL query that contains '>> WITH ORDER BY ' clause
- 221256: Before-after configuration gets overwritten after adding new tables and applying the new configuration by using the search filter
- 218419: Table-level permission changes are not captured in ApexSQL Audit reports when using 'SQL Audit' technology.
- 212247: Select statement is not audited using Extended Events auditing when it is executed via exec SQL command
- 225487: Missing extended event sessions not triggering "Missing extended event sessions" error
- 223696: Internal SQL Server events which do not contain a login and application name

are captured in the reports

- 223695: Previous auditing sessions are not successfully removed after switching the auditing technology causing events to be duplicated in reports
- 216473: Extended event session is not closed when auditing technology is switched from Extended events to Trace

Release: 2023.01.2212

Date: June 19, 2023

Enhancements:

- Additional logging is available by activating Debug mode.
- Additional processing of files from the ActiveSessions folder after encountering 3rd party parsing errors
- Creation of zipped files containing details about the queries which could not be processed
- Optimization of the Before-after trigger installation process for databases with a large number of Primary Key indexes.
- Support for hosting the Central Repository and auditing events for SQL Server 2022.

Fixes:

- 219140: API JSON output adds comma characters at the end when 'eventsPerPage' value from the URL is greater than 50,000.
- 220351: API call link cannot be opened in the browser (or used to generate data in power BI) when logged in as a user different to the one running ApexSQL Audit central.
- 221921: DML operations inside of a stored procedure are not audited when using Extended event data collection.
- 222518: The auditing configuration is not applied due to timeout being strictly defined as a 10-second value that is now set to follow global timeout settings.
- 222602: Application log messages are incorrectly labelled as INFO instead of ERROR when an error occurs while creating audit sessions.
- 222847: Package is not quarantined when a SQL Query operation type is not extracted correctly from query text data in a specific case.
- 223536: Cannot parse "Deny a permission to principal" operation when there are blank spaces at the end.
- 224205: An Extended event session file containing auditing data gets deleted by SQL Server when a very large number of operations is being executed
- 221223: 'Saving configuration was not successful' message is displayed when trying to exclude a local login in a domain environment
- 225537: SQL Audit auditing configuration is only partially applied when a database which doesn't exist anymore is included in the configuration filters
- 225485: Auditing configuration is only partially applied when there is an ApexSQL Audit Extended event session on SQL Server in stopped state
- 227648: 'Saving configuration was not successful' error is encountered when applying a Before-after configuration for an Availability Group

- 227647: 'Error connecting to server' is encountered when trying to add a database after an Availability group has been added for auditing
- 227557: Error 'Msg 10314, Level 16, State 11' is encountered when trying to update a table on the (new) primary AG replica after a failover
- 227466: SQL Audit database session is not properly created after a failover occurs in an Availability Group
- 228349: An Availability Group cannot be added via listener name if the FQDN of the listener is used
- 227237: AG cluster cannot be added via listener name if the name doesn't match the one given to the Availability Group
- 228615: Incomplete data after reading Microsoft Extended Event file using the MS function - fn_xe_file_target_read_file
- 228776: Auditing sessions are not properly created when a specific combination of filters is used
- 228590: The Before-after section of the UI is not responsive when adding a database with a large number of Primary Key indexes.
- 219710: 'Saving configuration was not successful' is displayed when trying to apply a Before-after configuration with a large number of tables and columns
- 229130: Tables are not successfully loaded in the Before-after configuration when adding a database with specific case-sensitive collation settings
- 229547: 'MERGE INTO' operation is captured as 4 events when using SQL Audit data collection
- 229583: 'DBCC CHECKDB' command is captured with a duplicate record when using SQL Audit data collection
- 229666: Continuous connection timeouts occur because the max pool size has been reached
- 229601: Extended event and SQL Audit sessions are improperly filtered on the SQL instance for all databases except the first one from ApexSQL Audit's configuration filters
- 229777: Auditing agent processes for Always On and FCI clusters are not successfully updated after an upgrade to a new version
- 229779: SQL Audit and Extended event sessions are not properly created when system databases are added for auditing

Changes:

- The column order of Before-after reports has been modified and is now displayed in alphabetical order. This modification enables a significant performance improvement both during the initial setup and when updating the configuration for Before-after auditing

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact

Technical Support Resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.


Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

Legend

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

 **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.