



AuditMaster User's Guide

Zen v16

Activate Your Data™

Copyright © 2023 Actian Corporation. All Rights Reserved.

This Documentation is for the end user's informational purposes only and may be subject to change or withdrawal by Actian Corporation ("Actian") at any time. This Documentation is the proprietary information of Actian and is protected by the copyright laws of the United States and international treaties. The software is furnished under a license agreement and may be used or copied only in accordance with the terms of that agreement. No part of this Documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or for any purpose without the express written permission of Actian. To the extent permitted by applicable law, ACTIAN PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, AND ACTIAN DISCLAIMS ALL WARRANTIES AND CONDITIONS, WHETHER EXPRESS OR IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OR OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT WILL ACTIAN BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ACTIAN IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

The manufacturer of this Documentation is Actian Corporation.

For government users, the Documentation is delivered with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013 or applicable successor provisions.

Actian, Actian DataCloud, Actian DataConnect, Actian X, Avalanche, Versant, PSQL, Actian Zen, Actian Director, Actian Vector, DataFlow, Ingres, OpenROAD, and Vectorwise are trademarks or registered trademarks of Actian Corporation and its subsidiaries. All other trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contents

Introducing Actian AuditMaster	1
What Is AuditMaster?	2
Features of AuditMaster	3
Where to Go Next.	4
Preparing to Install AuditMaster	5
General Installation	6
Installation Checklist	6
Precautions	6
Permissions and Privileges	7
Authorization License	7
Release Notes	7
Documentation	7
Customized Installation	8
Installer Executable	8
AMsetup.ini Settings	8
Installing AuditMaster	11
Before You Begin.	12
Installation Notes	12
Important Information about Upgrading from an Older Version	13
Hidden Administrative Share	15
Installing AuditMaster	16
Installing AuditMaster Control Center as a Client.	18
Common Questions After Installing AuditMaster	19
Removing AuditMaster	20
Getting Started with AuditMaster	23
Accessing AuditMaster	24
Connecting AMCC to AuditMaster on a Remote Zen Server	25
Changing Your User Password	26
Running AuditMaster under Zen Security	27
Additional Notes.	27
Using AuditMaster Control Center	29
AuditMaster Control Center Visual Reference	30

Menus, Toolbars, and Tabs	30
Audit Servers List	33
Audit Configurations.....	33
Audit Records Tab.....	34
Audit Record Details.....	34
Status Log Tab.....	35
Display Preferences.....	35
Working with Audit Configurations	37
Managing Schemas	39
Importing a Schema from a Zen Database	40
Removing an Audit Configuration	41
Configuring Data Monitoring With a Schema	42
Configuring Data Monitoring Without a Schema.....	44
Monitoring Items Other than Data Files	45
Operations to Audit by Table or File	46
Querying Audit Records	47
Displaying Audit Records.....	48
Running a Regular Query on the View File	48
Working with the Audit Records Tab	50
Reviewing Audit Data Columns	51
Viewing Audit Record Details.....	52
Running Queries	53
Displaying All Audit Records	53
Restricting a Query	53
Building an Advanced Query	56
Using the Files Group in Queries	60
Running a Saved Query or Last Query Executed	61
Working with Archived Audit Records	63
Manual Archiving	63
Managing Archives	64
Working with Alerts	66
Audit Alert Best Practices	68
Searching Audit or Log Records.....	70
Exporting Audit or Log Records to a Text File	72
Displaying Audit Records under Zen Security	73
Using AuditMaster Undo	74

Administering AuditMaster	75
Adding and Removing Servers	76
Adding a Server	76
Removing a Server	77
Reviewing Activity in the Status Log	78
Disabling and Enabling the Monitor	80
Maintaining Users	81
Maintaining Server Settings	83
Automatic Archiving	85
Errors to Audit	86
Operations to Audit Globally	86
Replacing the Network Share with a Local Path	88
 Basic Troubleshooting	 91
General Tips	92
Troubleshooting Strategies	93
Restarting the Status Log	94
No Records Returned by Query Despite Changes to Application Data	95
Database Engine	96
 Advanced Operations	 97
Querying Audit Data Directly through SQL	98
Query Data-Model Generator Utility	98
Creating a Virtual Database	99
The Structure of an Audit Record	101
Running a Query on the Current View File	104
Running a Query on an Archived File	104
Summary of Direct Query Methods	107
AuditMaster and Client-Side Caching	108

Introducing Actian AuditMaster

This documentation introduces you to Actian Zen AuditMaster, a monitoring and auditing application for Zen Enterprise Server and Cloud Server. It leads you through installation or upgrade, configuration steps, and then explains how to work with the application. Important topics include end-user and administrator tasks in Zen database environments, both with and without Zen security features enabled.

The following topics provide an overview of AuditMaster and its features.

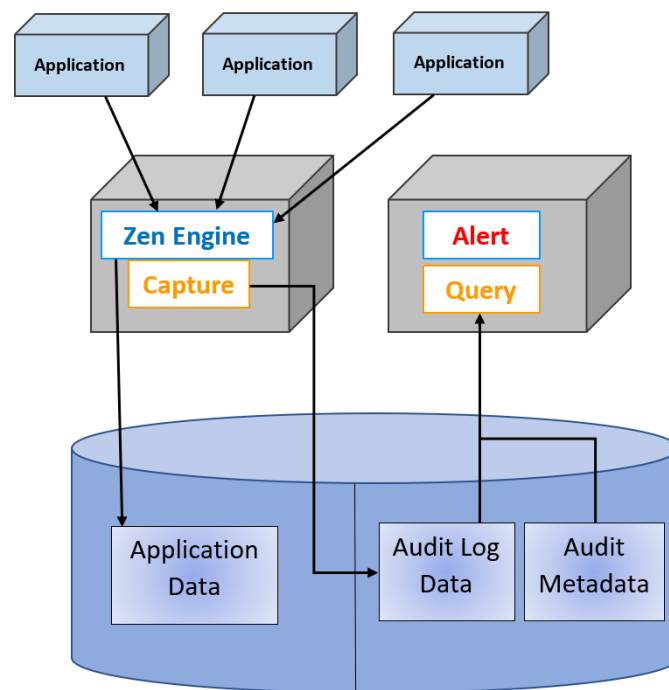
- [What Is AuditMaster?](#)
- [Features of AuditMaster](#)
- [Where to Go Next](#)

What Is AuditMaster?

AuditMaster is a transaction monitoring product for tracking access to and changes in data. It provides a detailed audit trail that captures the following information for every transaction in a database:

- Who accessed a record or performed a change
- What change took place
- When the access or change occurred
- Where the access or change originated
- How the change was made

AuditMaster monitors databases, not client applications. It logs access to the database as well as changes made to data, including the reading of records even if no change is made.



AuditMaster creates a comprehensive audit trail. Every time a record in a monitored data file changes, AuditMaster logs the record both before and after the change, making it possible to review data changes and, if desired, recover from errors.

Features of AuditMaster

To provide a secure audit trail, AuditMaster offers features to enable you to do the following:

- **A comprehensive logging system**
Capture events in your database and snapshots of database records before and after the events occur, whether transactions originate from third-party applications or within the Zen system.
- **A query builder**
Create, customize, and manage queries.
- **Alerts**
Use queries to run against events captured by AuditMaster and send event information to Windows system logging for various purposes such as security, administration, and notification.
- **Archive manager**
Store and retrieve your historical information, using data compression if needed.

Where to Go Next

The following topics may be of interest:

- To install the application, see [Preparing to Install AuditMaster](#).
- To learn about its operation, see [Getting Started with AuditMaster](#).
- To find troubleshooting instructions, see [Basic Troubleshooting](#).

Preparing to Install AuditMaster

The following topics cover a general or custom installation of AuditMaster:

- [General Installation](#)
- [Customized Installation](#)

General Installation

This topic covers the following information:

- [Installation Checklist](#)
- [Precautions](#)
- [Permissions and Privileges](#)
- [Authorization License](#)
- [Release Notes](#)
- [Documentation](#)

Installation Checklist

The following list helps you prepare for installation or upgrade. Before beginning, make sure your system meets the minimum hardware and software requirements for AuditMaster listed on the [Actian website](#).

Each checklist item is described in more detail in the topics that follow.

- ☐ You have taken the appropriate precautions before installing.
- ☐ You have full administrator-level permissions and privileges on the system where you plan to install.
- ☐ You have a license (unless you are testing with a trial version).
- ☐ You have access to the latest release notes.

Precautions

AuditMaster installation stops and restarts the Zen database engine. Install AM at a time acceptable to your operations.

Back up any important files on the target hard drive, including data files, before you proceed.

Before starting installation, disable any antivirus applications. These may be reenabled immediately after installation is complete. If you do not disable them, expect prompts to allow various installation tasks to execute.

Permissions and Privileges

To install AuditMaster, you need full administrator-level rights on the system where you are installing.

Authorization License

If you enter no license key during installation, you can audit data for an evaluation trial period. At the end of that time, AuditMaster will cease to monitor data. You will be able to query existing audit records captured during the trial period, although certain features may no longer be available.

To apply a license key, in Zen Control Center select **Tools > License Administrator** or open a command prompt and run either **clilcadm** for 32-bit installations or **w64clilcadm** for 64-bit installations. For more license key information, see *Zen User's Guide*.

No license key is required for the installation on a remote Zen Client system. The AMCC client by itself does not require a license.

Note: AuditMaster can run only if the Zen server instance it is monitoring has an active license.

Release Notes

We recommend that you read the release notes in the file `readme_am.htm` for product news that could not be included in the user documentation but may be needed for successful AuditMaster installation and use.

This file is posted on the [Actian website](#) and also located in the root directory of the AuditMaster download or the AuditMaster CD, as well as after installation in the default location `C:\Program Files (x86)\Actian\Zen\Audit\Docs`.

Documentation

AuditMaster includes this documentation under its Help menu. You can also open context-sensitive topics by pressing the F1 key in various places in the AMCC window and dialogs. An online version is posted at the [Actian documentation website](#). If you would like a PDF file for printing, you can download it from the [Actian distribution website](#).

Customized Installation

This topic covers the technology and customization settings used for AuditMaster installations. AuditMaster installation uses Microsoft Installer (MSI). The AMsetup.ini file contains default settings that you can change for custom installations.

Installer Executable

For most installation scenarios, the installer executable should be used. It is an InstallShield package that performs certain checks before installation. It also detects 32- or 64-bit Windows, launches the appropriate installation, and provides all 32- and 64-bit client components appropriate to your system.

The following table describes the AuditMaster installer on Windows operating systems.

Product	Installation Package	Description
AuditMaster Server	Install_AuditMaster.exe	<ul style="list-style-type: none">• Installs 32-bit engine on 32-bit operating system.• Installs 64-bit engine on 64-bit operating system.• Installs all client components.
AuditMaster Client	Install_AuditMaster.exe	<ul style="list-style-type: none">• Installs 32-bit client on 32-bit operating system.• Installs 64-bit client on 64-bit operating system.

AMsetup.ini Settings

The AMsetup.ini file contains all of the settings needed for a typical installation. This file is used by Install_AuditMaster.exe and is located in the same folder as the .msi file that uses it.

AMsetup.ini consists of a set of properties applied during installation. Comments in the file explain the settings and give all accepted values.

Caution! You must use the specific AMsetup.ini file included with the version of the product that you are embedding. Because installer technology and installation settings can change from version to version, the file must match the product that it accompanies.

The following table lists property settings in AMsetup.ini. The settings are grouped into categories. The value for each setting is contained in a key.

Categories	Keys
Directory Locations	PVSW_AM_INSTDIR32
	PVSW_AM_INSTDIR64
Destination Folder	PVSW_AM_SKIP_INSTALLDIR
Administrative Share Name	PVSW_AM_SHARE_NAME
License key	PVSW_AM_LICENSE_KEY
License key dialog	PVSW_AM_SKIP_LICENSE

Installing AuditMaster

The following topics explain how to install or upgrade AuditMaster:

- [Before You Begin](#)
 - [Installation Notes](#)
 - [Hidden Administrative Share](#)
 - [Important Information about Upgrading from an Older Version](#)
- [Installing AuditMaster](#)
- [Installing AuditMaster Control Center as a Client](#)
- [Common Questions After Installing AuditMaster](#)
- [Removing AuditMaster](#)

Before You Begin

We recommend reading the following before installing or upgrading AuditMaster:

- [Preparing to Install AuditMaster](#) for system requirements and platform-specific notes.
- The release notes (readme_am.htm) for information not included in the user's guide. This readme file can be found at the [Actian website](#).

These topics provide additional information before installation:

- [Installation Notes](#)
- [Important Information about Upgrading from an Older Version](#)
- [Hidden Administrative Share](#)

Installation Notes

Be aware of the following before installing AuditMaster on any platform:

- You must have full administrator-level rights on the system where you install AuditMaster.
- We recommend you disable antivirus applications. These may be reenabled immediately after installation. If you do not disable them, expect prompts to allow installer tasks to execute.
- The Zen database engine is stopped and restarted during AM installation. Choose a time acceptable to your operations.
- If you are installing AMCC to access a Zen server when security is enabled and security policy is set to either Mixed or Database, see [Running AuditMaster under Zen Security](#). Prepare to set up AM in a Zen secure environment by reviewing security features in *Advanced Operations Guide*. Note that for installation with database security enabled, you must select the **Prompt for Client Credentials** setting in Zen Control Center (ZenCC) in the **Properties > Access** window for the Zen engine.
- Installation creates a log file in the installing user's %temp% directory, where *nn* refers to the version:
 - On 32-bit systems, Zen_vnn_AuditMaster_x86_Install.log
 - On 64-bit systems, Zen_vnn_AuditMaster_x64_Install.log
- The 32-bit installer SetupAuditMaster32_x86.exe is not supported on 64-bit Windows.

Important Information about Upgrading from an Older Version

Action has renamed PSQL to Zen. This renaming has resulted in new locations for AuditMaster files. To upgrade to AuditMaster 15, if you do not need your existing audit records, configurations, queries, and alerts, then all you need to do is remove the earlier AuditMaster version before installing AuditMaster 15. In the new installation, you will then create new audit configurations, queries, and alerts. Only new audit records can be queried, and previously captured audit records are no longer accessible.

On the other hand, if you wish to continue using everything in the earlier installation, then you must manually back up copies of certain file directories for reuse in the AuditMaster 15 installation. The overall steps are as follows:

1. Copy and save certain existing AuditMaster file directories.
2. Remove AuditMaster.
3. Upgrade to Zen v15.
4. Install AuditMaster 15.
5. Copy the saved files to their location in AuditMaster 15.

These tasks require starting and stopping the Zen database engine. Choose a time to do so most convenient to your data operations. Here are the detailed steps:

1. Create a directory in a backup location, such as %temp%\AM_Save.
2. Stop all database services.
3. Find the AuditMaster share location in your existing installation. Here are the default locations:
 - In 64-bit Actian Zen (PSQL) v14, the default is C:\Program Files (x86)\Actian\PSQL\Audit.
 - In 64-bit Actian Zen (PSQL) v13, the default is C:\Program Files (x86)\Actian\PSQL\Audit.
 - In 64-bit Actian PSQL v12 and earlier, the default is C:\Program Files (x86)\Pervasive Software\PSQL\Audit.
 - In 32-bit Actian Zen (PSQL) v14, the default is C:\Program Files\Actian\PSQL\Audit.
 - In 32-bit Actian Zen (PSQL) v13, the default is C:\Program Files\Actian\PSQL\Audit.
 - In 32-bit Actian Zen (PSQL) v12 and earlier, the default is C:\Program Files\Pervasive Software\PSQL\Audit.

-
4. From this directory, copy the following folders to the backup location you created in the first step:
 - Arch
 - Comp
 - DATA
 - Empty
 5. You can now restart all database services while continuing with the rest of the steps given here.
 6. If you are using a custom installation location for your existing AuditMaster installation and plan to use it again in AuditMaster 15, we suggest you write down the location for reuse in AuditMaster 15.
 7. Whether a default or custom location, this share is given the default name PVSWAUDIT\$. If you are using a custom share name, then the same one must be used in AuditMaster 15. To find the share name, run `net share` at a prompt to return information similar to the following:

```
PVSWAUDIT$ C:\ProgramData\Action\Zen\Au... Automatically created by AM
```

This example shows the default share name. A custom name will be whatever was assigned. If the path name displayed is too long, as shown here, run `net share <share name>` to see the entire path.
 8. Remove AuditMaster.

When you are prompted to remove all data and configuration settings, choose to leave them rather than remove them. In the installer wizard, this means **not** selecting the check box to remove them.
 9. Upgrade to Zen v15.
 10. Install AuditMaster 15 using the steps under [Installing AuditMaster](#). If you are using a custom share name, to use the same value that you wrote down from the previous AuditMaster installation.
 11. After installing AuditMaster 15, stop the Zen v15 database engine service.
 12. Copy the backups of Arch, Comp, DATA, and Empty folders to C:\ProgramData\Action\Zen\Audit in the AuditMaster 15 installation, allowing them to overwrite existing folders and their contents.
 13. Restart the Zen v15 database engine.

-
14. Start AuditMaster Control Center (AMCC) and confirm that the configuration settings from your previous installation are working as expected and that you can view audit records. If so, then you can delete the folders in both the backup and the previous installation.

Hidden Administrative Share

When you install AuditMaster on a Zen server, the default installation settings create a hidden administrative share to certain AM components. By default, the share name is PVSWAUDIT\$ for the path C:\ProgramData\Actian\Zen\Audit, but the share name can be set to another value during installation. Also, it is not required that the share be hidden. In using the share, you may need to consider the following things:

- When you install AMCC on a remote client, you must provide the client system with access to this share on the server. For details, see [Accessing AuditMaster](#).
- For AuditMaster to work successfully, you may need to register the share with your firewall system.
- To meet security requirements, the share can be replaced with an explicit local path name. Doing so blocks remote clients and restricts access to only the local system. For instructions, see [Replacing the Network Share with a Local Path](#).

Installing AuditMaster

AuditMaster has two parts: A server monitor and a viewer client called AuditMaster Control Center (AMCC). On Zen Enterprise Server or Cloud Server, the monitor and AMCC are installed together. On Zen Client, Reporting Engine, or Workgroup, AMCC will be installed by itself to connect to an AuditMaster server monitor on a remote Zen server to display its audit records.

An AuditMaster license authorizes one server installation, but you can install as many clients as needed across your network environment. For instructions, see [Installing AuditMaster Control Center as a Client](#).

You must run the AuditMaster installer on the system where you are installing it. You cannot run the installer from another system to install AuditMaster locally.

Note: The Zen database engine is stopped and restarted during AM installation. Choose a time acceptable to your operations

To install AuditMaster

1. Log on to the system with administrator rights.
2. Launch the installer program in one of the following ways:

If using...	Do...
Downloaded files	Open Install_AuditMaster.exe in the download directory.
CD	Insert the CD. If installation does not start, open Install_AuditMaster.exe on the CD.

3. In the Welcome page, click **Next**.
4. For **License Agreement**, accept the terms and click **Next**.
5. For **License Key**, enter an AuditMaster license key and click **Next**. If you enter no key, your trial period starts now. Without a license, you can audit for the trial period. After that, auditing ends, but you can still query and view already logged audit records. For more information, see [Authorization License](#).
6. For **Installation Folders**, if needed you can change the default locations. Note that for 64-bit environments, both the 32- and 64-bit components must be on the same system where a Zen server runs and must be installed to different locations. After you make any changes, click **Next**.

-
7. For **Share Name**, the installer asks for a share name to assign to the AuditMaster data directory path. Accept the default share name **PVSWAUDITS** or enter a different one according to your IT needs, and click **Next**.
 8. The installer is now ready to install the program. You can click **Back** to change settings or click **Install** to continue.
 9. When installation is complete, click **Finish**.

You can now open AuditMaster and connect to a Zen server, as described in [Accessing AuditMaster](#).

Installing AuditMaster Control Center as a Client

AuditMaster automatically installs its Control Center client (AMCC) on a Zen server. You may also install it alone on Zen Client, Workgroup, and Reporting Engine systems. Once installed on these systems, AMCC can then connect to AuditMaster on a Zen server as a remote client to work with audit records.

To install AMCC as a client

Zen Client, Workgroup, or Reporting Engine must be already installed and configured on the system where you install AMCC as a client.

1. Log on to the system with administrator rights.
2. Launch the installer program in one of the following ways:

If using...	Do...
Downloaded files	Open Install_AuditMaster.exe in the download directory.
CD	Insert the CD. If installation does not start, open Install_AuditMaster.exe.

3. In the Welcome page, click **Next**.
4. For **License Agreement**, accept the terms and click **Next**.
5. For **Installation Folder**, if needed you can change the default location. After you make any change, click **Next**.
6. The installer is now ready to install the program. You can click **Back** to change settings or click **Install** to continue.
7. When installation is complete, the installer displays a notice. Click **Finish**.

You can now connect to AuditMaster on a Zen server, as described in [Accessing AuditMaster](#).

Common Questions After Installing AuditMaster

The following items contain answers to question you may have after running the installation program.

Where are the AuditMaster release notes?

The readme_am.htm file is available in three places:

- On the [Actian website](#).
- Installed with the product. The default location is C:\Program Files (x86)\Actian\Zen\Audit\Docs.
- In the root directory of the AuditMaster installer.

Do I have to configure anything in Zen Control Center (ZenCC) for AM?

No. AuditMaster requires no special settings in ZenCC. All settings and configuration are done in AMCC with the exception of the Prompt for Client Credentials option if the Zen server has Btrieve security enabled.

Does the AuditMaster installation create a log file?

Yes. Installation creates a log file in the installing user's %temp% directory, where *nn* is the version:

- On 32-bit systems, Zen_vnn_AuditMaster_x86_Install.log
- On 64-bit systems, Zen_vnn_AuditMaster_x64_Install.log

Does an upgrade retain AuditMaster data, queries, and settings?

Yes, so long as you follow the instructions under [Important Information about Upgrading from an Older Version](#).

Removing AuditMaster

Uninstalling AuditMaster removes its components in the Audit directory of its installation location. Files in other locations are untouched and can be reused if you reinstall AM in the same location.

Note: AM removal stops and restarts the Zen database service. Choose a time acceptable to your operations.

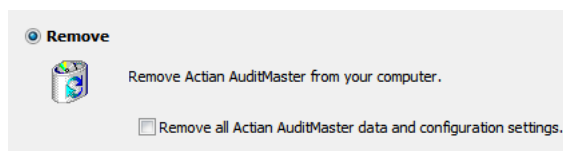
To remove AuditMaster

AuditMaster can be removed in the normal way from Windows Control Panel. It is listed as Actian AuditMaster 15.

To reinstall AuditMaster and continue using existing data and settings

If you plan to reinstall AuditMaster and want to continue using the existing audit data, configuration settings, queries, and alerts, follow these steps:

1. Before you begin removing AuditMaster, find its installation. The default location is C:\Program Files (x86)\Actian\Zen\Audit. In a custom installation, the location of this Audit directory may differ. If so, then note the location so that you can select it when you reinstall AuditMaster.
2. When you remove AuditMaster, be sure that you do **not** select the check box to remove existing audit data, configuration settings, queries, and alerts. Leave the default setting clear as shown in the following figure:



3. So long as you do **not** select this check box, you will be able to do one of the following:
 - Reuse the previous installation location when you reinstall AuditMaster.
 - Install AuditMaster in a new location and then copy any custom Audit folders to the Audit directory in the new installation.
 - Upgrade from AuditMaster 14 or earlier to AuditMaster 15 or later and migrate existing audit data, configuration settings, queries, and alerts to the upgrade installation. This method is covered in detail in [Important Information about Upgrading from an Older Version](#).

To remove AuditMaster from a client

Removing AuditMaster on a client is the same as removing it on a server.

To view the AuditMaster removal log

Removing AuditMaster creates the following log file in the current user's %temp% directory:

Zen_v15_AuditMaster_Repair_Remove.log

Getting Started with AuditMaster

The following topics cover considerations for general usage:

- [Accessing AuditMaster](#)
- [Changing Your User Password](#)
- [Running AuditMaster under Zen Security](#)

Accessing AuditMaster

AuditMaster Control Center requires authentication with a user name and password. The type of account determines access to audit records and the availability of AMCC menu commands:

- **User**
A regular user is able to query and view logged audit records and manage audit record archives.
- **Administrator**
In addition to regular user privileges, an AuditMaster administrator can manage users, view the status log, create audit configurations, adjust system settings, and create alerts.

The built-in AM administrator account has the user name **admin** with the initial password **MASTER**. Passwords are case-sensitive, while user names are not.

We recommend that you change the AM admin password. To do so, see [Changing Your User Password](#). Note that the admin account and all user logins within AuditMaster are internal only and unrelated to network, local operating system, or database user logins used by Windows or Zen.

For more information on the relationship of AuditMaster logins to Windows and Zen database logins, see [Running AuditMaster under Zen Security](#) and [Displaying Audit Records under Zen Security](#).

To log in to AuditMaster

1. In AMCC, right-click an audit server name and select **Login**, or expand that server node.
2. In the login dialog, enter an AuditMaster user name and password and click **OK**.

If this is the first login after installation, you must do so as the AuditMaster admin user.

The next task is to set up data monitoring, as described in [Working with Audit Configurations](#).

To log in from Zen Client

You can use these same steps after you create a connection from AMCC on Zen Client to AuditMaster on a Zen server. To create this connection, follow the instructions below.

Note: For AuditMaster on a Zen server to recognize your login from AMCC on Zen Client, you need to be logged in to the Windows system under an account authenticated by both the network and also the Zen server, depending on its database security settings. For more information, see [Displaying Audit Records under Zen Security](#), as well as security topics in *Advanced Operations Guide*.

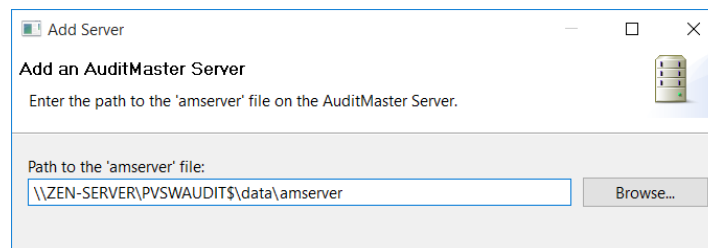
Connecting AMCC to AuditMaster on a Remote Zen Server

When you install AuditMaster on a Zen server, the host system is automatically added to the Audit Servers list in AMCC. For AuditMaster on Zen Client, Workgroup, or Reporting Engine, use the following steps to connect remotely to AuditMaster on the Zen server. For information about client access to a Zen database server with security policy set to either Mixed or Database, see [Running AuditMaster under Zen Security](#).

1. On the client system, make sure that Zen Client, Workgroup, or Reporting Engine is installed.
2. On the client system, open AMCC and select **Server > Add** or click the **Add Server** link in the Welcome tab.
3. In the Add Server dialog, use one of the following to enter the path to the AuditMaster file **amserver**.
 - The name of an accessible Zen server. You can browse for this name on your network.
 - The full name for this system, such as zen-server.englab.local.
 - The IP address for this system.

In a default installation, amserver is in `\\<server>\PVSWAUDIT$\DATA`.

4. The path to the amserver file should resemble the following:



5. Click **OK** to add the system to the Audit Servers list.
6. Right-click the newly listed server and select **Login**, or expand its node.
7. In the Login dialog, enter an AuditMaster user name and password and click **OK**.

Typically, the next task is to set up data monitoring, as described in [Working with Audit Configurations](#) or to run a query if tables or files are already being monitored.

Changing Your User Password

AuditMaster access is password-protected. While logged in to a server, you can change your password for that server only. Your AuditMaster password for each server you access is specific to that server, even if the same user name is used.

To change your password

1. In AMCC, log in to a server.
2. Select **Server > Change Password**.
3. In the Change Password dialog, enter your **current password**.

The password is case-sensitive and can be up to 40 characters long. For double-byte character sets, the maximum length is 20 characters.

4. Enter the **new password** in both fields provided and click **OK**.

Your password is changed.

The built-in administrator account has the user name **admin** and the initial default password **MASTER**. We recommend that you change the administrator password. Note that the AM administrator account and all user accounts are internal to AuditMaster and unrelated to network, operating system, or database user logins used by Windows or Zen.

For more information on the relationship of AuditMaster logins to Windows and Zen database logins, see [Running AuditMaster under Zen Security](#) and [Displaying Audit Records under Zen Security](#).

Running AuditMaster under Zen Security

AuditMaster is compatible with all Zen database security settings. AuditMaster installation adds the AuditMaster internal database to the Zen DefaultDB data directory list. After installation, the security settings in DefaultDB provide the same protection for the AuditMaster database.

The following table summarizes typical security settings. The first two rows give the settings, the next two rows describe logins and permissions, and the last row lists the protection provided.

Security	Classic	Mixed	Database
Database Security on DefaultDB	On	On	On
Btrieve Security on DefaultDB	Off	On	On
Authentication in AMCC	AuditMaster login	<ul style="list-style-type: none">• AuditMaster login• OS or network login	<ul style="list-style-type: none">• AuditMaster login• Zen login
Database User Needed	None	<ul style="list-style-type: none">• Zen user under DefaultDB. Must match OS or network login.• Zen user must have at least Select permission to run existing queries• To create and save new AuditMaster queries, Zen user must have Update and Insert rights.	<ul style="list-style-type: none">• Zen user under DefaultDB• Zen user must have at least Select permission to run existing queries• To create and save new AuditMaster queries, Zen user must have Update and Insert rights.
What is protected?	AuditMaster access	<ul style="list-style-type: none">• AuditMaster access• Audit data and .ddf files• ZenCC SQL Editor access• Btrieve file access	<ul style="list-style-type: none">• AuditMaster access• Audit data and .ddf files• ZenCC SQL Editor access• Btrieve file access

Additional Notes

- AuditMaster and Zen logins are separate and unrelated authentications, even though in some cases AMCC presents a single dialog to enter both because both are needed at that time.

-
- When you have Database security policy under DefaultDB and you want to use AMCC from a remote client, in PCC you must enable **Prompt for Client Credentials** under **Properties > Access** for the Zen server engine. This setting provides a login dialog in AMCC for the remote user.
 - After installing AuditMaster, if you need to change Zen security policy, first close all AMCC clients. Failing to do so results in Zen returning status code 94 permission errors.
 - If you are not currently using Btrieve Mixed or Database security and you enable it only to increase AuditMaster security, keep in mind that DefaultDB is a global configuration and applies to all transactional Btrieve applications using Zen. Enabling security for AuditMaster may require changes to how you manage access to Zen or Btrieve data.

See also [Displaying Audit Records under Zen Security](#). For more information on database operations in a Zen security environment, see *Advanced Operations Guide*.

Using AuditMaster Control Center

AuditMaster Control Center (AMCC) is the user interface for the AuditMaster application. Its window displays a list of Zen server installations configured for AM monitoring. As you work with monitoring tasks, it provides various information and options.

A Zen server database where AuditMaster is installed and running is called an audit server. The monitor reads database activity and logs audit records which can then be queried and displayed in the AMCC client.

The data tree represents your auditing system. Each branch of the tree holds an AuditMaster server and its current view file, archive files, and saved queries. For more information, see [AuditMaster Control Center Visual Reference](#).

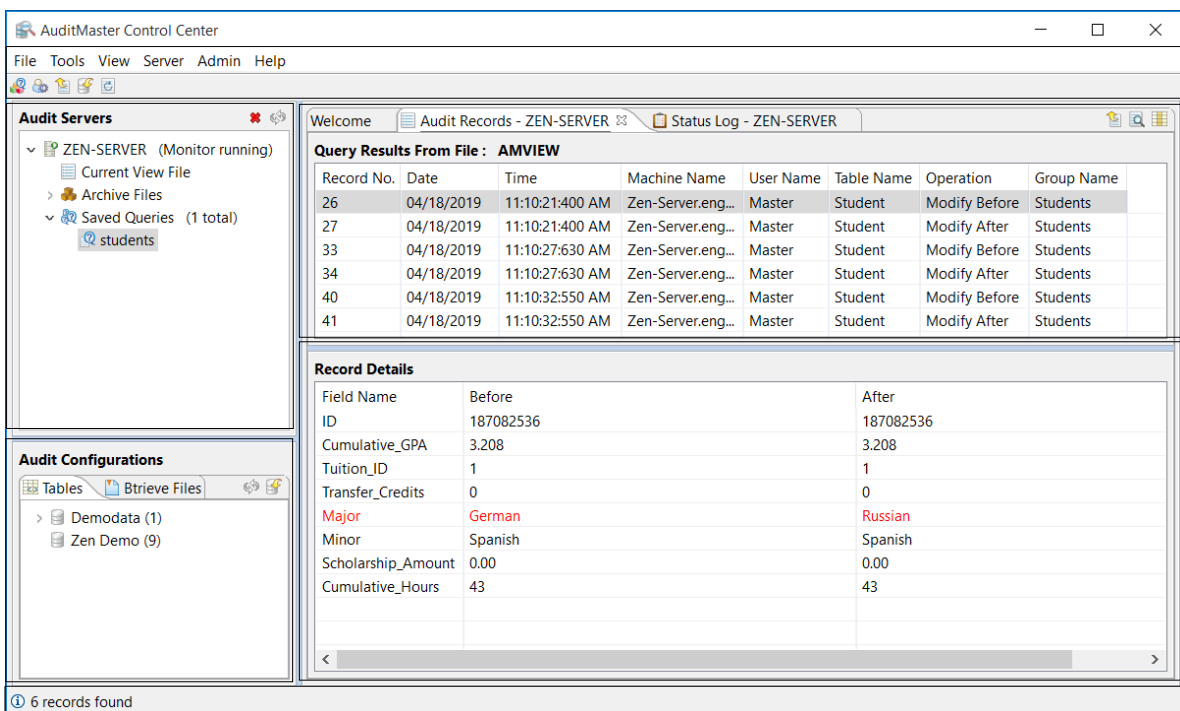
AuditMaster Control Center Visual Reference

Once you have logged in as a user and run a query to display audit records, the AuditMaster Control Center (AMCC) window should resemble the following example, which shows the monitoring of records in the Demodata sample database.

The following topics provide more information on how to use AMCC:

- [Menus, Toolbars, and Tabs](#)
- [Audit Servers List](#)
- [Audit Records Tab](#)
- [Audit Record Details](#)
- [Status Log Tab](#)
- [Display Preferences](#)

For details, click any item in the list, or click an area of the following example:









Menus, Toolbars, and Tabs




To learn about AMCC menu and toolbar options, click a menu name, icon, or tab in the following images for the main window and the tabs that display query results and log information.

File Tools View Server Admin Help



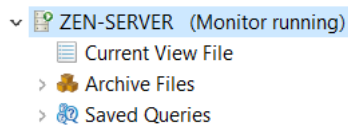
Menu or Toolbar	Command	Description
File	Query or 	Opens Query Builder to search for records. A query may be based on user, date, action, and other criteria. For details, see Querying Audit Records .
	Advanced Query	Opens Advanced Query Builder to create more complex queries that cannot be built using Query Builder. For details, see Building an Advanced Query .
	Exit	Select Exit to log out and close AMCC.
Tools	Search or 	Searches for specific text in the Audit Records tab. For details, see Searching Audit or Log Records .
	Export or 	Exports a current or archived view file to a text file. For details, see Exporting Audit or Log Records to a Text File .
	Import Schema or 	Imports DDF information to use in displaying the contents of logged records. For details, see Importing a Schema from a Zen Database .
	Manage Archives	Opens a window for managing archived audit records. For details, see Managing Archives .
View	Preferences	Opens a window for setting the appearance of tabs and the number of archives listed. For details, see Display Preferences .

Menu or Toolbar	Command	Description
Server	Add	Creates a connection from an AMCC client to an AuditMaster server. For details, see Accessing AuditMaster .
	Remove	Removes an AuditMaster server connection. The server continues to capture new audit records, but the client cannot currently access them, although it still can query and display records already in its current view and archive files.
	Update Current View File or 	Refreshes the current view file from the audit log so that queries display the most up-to-date audit records.
	Change Password	Changes the password for the user currently logged into an AuditMaster server. For details, see Changing Your User Password .
Admin Available only to administrative logins	View Status Log	Displays the status log of AuditMaster activity.
	Server Settings	Maintains paths and other system settings for an AuditMaster server.
	User Maintenance or 	Allows you to add or remove AuditMaster users.
	Manage Alerts	Builds an alert based on a query (e.g., a certain user has made a change or a check is drawn for more than \$10,000). A tripped alert flags the monitored record with a bell icon 🔔 and writes an entry to the Windows Application event log. For details, see Working with Alerts .
Help	Contents	Provides an online version of the user's guide.
	AMCC Log	Open the event log.
	Clear AMCC Log	Clear the event log.
	About	Displays AuditMaster and Java version information.

Menu or Toolbar	Command	Description
Icons with no menu command	Filter 	Filter the status log messages displayed by type and date.
	Refresh status messages 	Updates the list of logged status and error messages in the Status Log tab.
	Select Columns to Display 	Select the columns to display when viewing audit records. For details, see Working with the Audit Records Tab .

Audit Servers List

The Audit Servers panel lists instances of Zen servers where AuditMaster is installed. The server names are the names of the machines. Each server name expands to show details. You can right-click icons for various command options. Queries may be run against either the current view or archive files or a combination. Saved queries are listed for reuse. *Monitor* refers to the AuditMaster feature that captures database activity.



Audit Configurations

An audit configuration is a set of one or more groups of database tables or Btrieve files to be monitored for activity. The Audit Configurations panel has two tabs: One for database tables and one for Btrieve files. For details, see [Working with Audit Configurations](#).

Audit Records Tab

When a query is run against the current view or an archive file, the Audit Records tab shows the query results.

Audit Records - ZEN-SERVER					
Query Results From File : AMVIEW					
Record No.	Date	Time	Table Name	Operation	Machine Name
35	09/13/2019	12:56:26:220 PM	n/a	Begin Trans...	Zen-Server.englab.local
36	09/13/2019	12:56:26:220 PM	Student	Insert	Zen-Server.englab.local
37	09/13/2019	12:56:26:220 PM	n/a	End Transa...	Zen-Server.englab.local

Audit Record Details

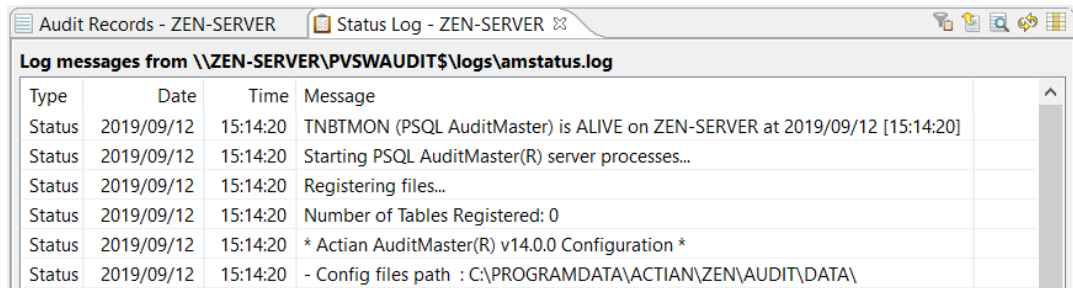
Audit records capture both database activity and AuditMaster operations. For database activity, the audit record detail area in the lower part of the AMCC window shows the fields of the data record where activity occurred.

Record Details	
Field Name	Field Value
ID	998451272
Cumulative_GPA	3.600
Tuition_ID	4
Transfer_Credits	0
Major	Biology
Minor	Statistics
Scholarship_Amount	5000.00
Cumulative_Hours	48

Note: Data record detail may be human readable or in hexadecimal, depending on whether the database schema has been imported for AuditMaster to use to display data. For details, see [Working with Audit Configurations](#).

Status Log Tab

The Status Log tab can be displayed by selecting **Admin > View Status Log**. This log displays AuditMaster activity, rather than activity in the database being monitored.



Type	Date	Time	Message
Status	2019/09/12	15:14:20	TNBTMON (PSQL AuditMaster) is ALIVE on ZEN-SERVER at 2019/09/12 [15:14:20]
Status	2019/09/12	15:14:20	Starting PSQL AuditMaster(R) server processes...
Status	2019/09/12	15:14:20	Registering files...
Status	2019/09/12	15:14:20	Number of Tables Registered: 0
Status	2019/09/12	15:14:20	* Actian AuditMaster(R) v14.0.0 Configuration *
Status	2019/09/12	15:14:20	- Config files path : C:\PROGRAMDATA\ACTIAN\ZEN\AUDIT\DATA\

The icons at upper right enable you to work with the status log entries by filtering them by type and date, exporting log messages as text files, searching for strings, refreshing the tab, and choosing which columns to display in the tab. The columns shown in this example are a few of the ones possible. For more information, see [Reviewing Activity in the Status Log](#).

Display Preferences

You can set the number of items displayed in the Audit Servers tree under Archive Files. You can also set options to save adjustments you make to the display of columns in the Audit Records and the Status Log tabs. To open the Preferences dialog for these settings, select **View > Preferences**. In the dialog under Table Layout, you can choose which settings to keep from session to session.

Working with Audit Configurations

AuditMaster captures audit data based on audit configurations. An audit configuration combines several things:

- An AuditMaster server installed with a Zen server engine
- If available, a schema imported from a Zen database
- One or more groups of files to monitor

Schemas are not required to run AuditMaster, but they make audit records human-readable as rows within tables. They also allow for more precise alerts.

When you import a schema into AuditMaster, all groups created under that schema can monitor tables that use it. In fact, when you browse for tables to add, only tables that use the schema are shown.

If you do not import a schema, you still must create a group for Btrieve files to be monitored. When you browse for files, only Btrieve files are shown.

Although you can create a single group and then add all monitored files to it, doing so may make it harder to plan the auditing you want to do. Creating more than one group, or even groups under separate imported copies of the same database schema, can simplify auditing activities.

For example, if you monitor different files for different customers, you can create a group for each customer, under which all files are for that customer. You can also import the same schema for each customer, under which all groups are for that customer. Your arrangement of imported schemas, groups, and files serves only to organize your thinking and has no affect on the audit records logged, nor on the database operations that generate them.

In summary:

- Each imported schema has one or more groups. Each group has one or more tables to monitor.
- Under an imported schema, all groups of monitored tables use only that schema.
- To monitor a Btrieve file with no schema, you must create a group where it can be added.
- A table or file can belong to only one group. Once added to a group, no other group can monitor it.

We recommend you step through the following examples to see how these concepts work in practice. It will work best to use the examples in the order given.

1. [Managing Schemas](#)

-
2. [Configuring Data Monitoring With a Schema](#)
 3. [Configuring Data Monitoring Without a Schema](#)
 4. [Operations to Audit by Table or File](#)

Managing Schemas

Zen data dictionary files (DDFs) provide the schema information that AMCC uses to make captured audit data human-readable and to enable querying at the field level in records. When you import a database schema in AMCC, it reads the DDFs from the data file directories for the database and stores them in its own database for use in displaying and querying audit data.

Without DDFs, data records captured from monitored files appear as hexadecimal rows, and you cannot query on specific data values. Lacking DDFs to format the display of a logged record, AuditMaster displays the insert of a record in a data file something like the following:

Record Details	
Offset	Data
	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F [0123456789ABCDEF]
00000000	62 39 6d 39 00 00 00 00 00 03 52 0f 05 00 00 00 [b9m9ppppppRppppp]
00000010	00 00 01 2f 00 45 6e 67 69 6e 65 65 72 69 6e 67 [ppp/pEngineering]
00000020	20 20 20 20 20 20 20 20 20 00 4d 61 74 68 20 20 [pMath]
00000030	20 20 20 20 20 20 20 20 20 20 20 20 20 00 00 [pp]
00000040	00 00 00 00 00 00 00 00 0f 00 24 00 [pppppppppp\$pp]

After schema import, AuditMaster can display the next logged record insert in a readable form like the following:

Record Details	
Field Name	Field Value
ID	998451272
Cumulative_GPA	3.600
Tuition_ID	4
Transfer_Credits	0
Major	Biology
Minor	Statistics
Scholarship_Amount	5000.00
Cumulative_Hours	48

Importing a schema does not change the display of records already captured. Records captured before schema import continue to appear as hexadecimal characters. In the same way, removing a schema has no effect on records logged while the schema was in use, which remain readable when they are displayed in AMCC. The display of records depends on whether a schema was imported during the time the records were logged.

Note: If you import the schema of a database that uses V2 metadata, and the DDF name for a table, column, or index is longer than 40 characters, AuditMaster displays only the first 40 characters. This shortened display of the table name, does not affect AM operation but may limit your ability to read some reports in the AMCC window.

The rest of this tutorial on schemas covers the following tasks:


-
- [Importing a Schema from a Zen Database](#)
 - [Removing an Audit Configuration](#)

Importing a Schema from a Zen Database

The following example shows how to import a schema.

Note that in AMCC in the Audit Configurations tab, an imported schema named Zen Demo has been installed with AuditMaster. It is the schema for the sample Demodata database. While it can be used, for the purpose of this example, the Demodata schema is imported again in a new audit configuration.

To import a schema from a Zen database

1. Select **Tools > Import Schema** or click the **Import Schema** button  in the toolbar to open the Import Schema dialog box. The dialog lists databases on the Zen server that can be used to create an audit configuration.
2. Select the **database** from the list whose schema defines the tables you wish to monitor.
3. The database name is automatically entered in the **Name** field for the new audit configuration. You can replace it with a different name. All keyboard characters are allowed, including spaces. This name will be associated with each audit record captured for this schema.
4. Enter a **description** for the audit configuration. All keyboard characters are allowed, including spaces. This string will appear in the properties for the audit configuration.
5. Enter a **version** for the audit configuration. All keyboard characters are allowed, including spaces. This version will be associated with each audit record captured for this schema.

AMCC displays the value you enter in parentheses after the audit configuration name. Use the version to suit your needs. The only restriction is that the version must be unique for each copy of the schema that you import.

6. Click **Import**.

The name you chose appears as an audit configuration and version at lower left in the AMCC window. You can now add and monitor groups of tables that use the imported schema.

Keep in mind the following things about imported schemas:

- When you import a schema to create an audit configuration, AuditMaster reads table and column information from the DDFs of the database and stores it internally within AuditMaster. If the database schema is later revised, and it no longer matches the one

imported into its audit configuration, then any query you run against audit records is likely to return truncated data or worse. To continue auditing the database correctly, you must import the schema into a new audit configuration and add the monitored files there. Regular queries created in Query Builder should continue to work for records captured in the new audit configuration. However, because Advanced Query Builder can search for data field information, you may need to recreate advanced queries to run against audit records captured after the database schema changed.

- If you have set Zen security policy on the DefaultDB database to Mixed or Database, then before working with a new schema for an audit configuration, you must add its path to the list of data locations for DefaultDB. See details under [Running AuditMaster under Zen Security](#).

Removing an Audit Configuration

Removing an audit configuration deletes the imported schema, its groups, and lists of monitored tables under those groups. The specified tables will stop being monitored the next time the Zen database engine is restarted.

To remove an audit configuration

1. In the Audit Configurations tab, right-click the name of an audit configuration and select **Delete**.
2. Confirm the deletion by clicking **Yes**.

The files that were monitored in the deleted groups are now available to add to groups in other audit configurations. Generally, you probably would need to remove an audit configuration only when a database schema changes. You would then import the new schema and recreate the groups and added files to monitor.

Configuring Data Monitoring With a Schema

This scenario shows how to set an audit configuration to monitor a group of one or more tables in a database that has data dictionary files (DDFs). It uses the Demodata sample database, which is installed with a Zen server. It also uses an existing audit configuration installed with AuditMaster, which already has the Demodata schema imported.

To create your own audit configuration, you must be an AuditMaster administrative user.

As explained in [Managing Schemas](#), schema information in DDFs makes audit records human-readable and enables you to query for particular data values.

A separate example under [Configuring Data Monitoring Without a Schema](#) shows how to monitor data files that do not have DDFs.

To use an audit configuration with a schema

1. Start AMCC to open the AuditMaster window, showing the available server.
2. Right-click the server name to select **Login**. You may also simply expand the name to open the login dialog.
3. Enter the default user name **admin** and the password **MASTER**. If you have changed the user name and password, enter those instead.

Note: The built-in user ID **admin** has the default password **MASTER**. Passwords are case-sensitive, but user names are not. This user ID and password are known only within AuditMaster and are unrelated to user accounts under Zen or Windows security.

4. Click **OK**.
5. Under Audit Configurations in the Tables tab, right-click the existing audit configuration **Zen Demo (9)** and select **Add Group**.
6. Enter the group name **Demodata**, and click **OK**.

Group names are not case-sensitive and can use any keyboard characters, including spaces, up to 40 characters in length. Although it is possible to reuse a group name from another audit configuration, we recommend a unique name to lessen risk of confusion when you build AuditMaster queries that use group names.

7. In the Browse Tables window under the Available Tables area, browse to the location of tables to associated with the schema for this audit configuration.

For this example, select the directory for Demodata, the Zen demonstration database. In a default Zen installation, this location is C:\ProgramData\Actian\Zen\Demodata.

8. Click the table named **Billing**, and click **Select** to move it to the Tables to Be Monitored list.

You can also click **Select All** to add every table in the current location.

Each table can be a member of only one group in any audit configuration. If you do not see a table where you expect it to be, check other groups in this and other audit configurations to see if it is already being monitored.

To remove an item from Tables to Be Monitored, select it and click **Remove**. Clicking **Remove All** drops all tables from the group.

Note: Any query or alert based on a removed table will now fail to find audit records and will also need to be deleted and, if needed, recreated after the table has been added to another group. If the table is added back to the same group as before, the query or alert will again succeed.

9. When you are finished selecting tables for the group, click **OK**.

The window closes and AMCC prompts you to restart the Zen database engine.

10. Click **Yes**.

After the restart, monitoring begins. In the Audit Configurations tab, the new group appears with the table listed under it.

11. If you wish to make changes, right-click the group and select **Edit**.

Configuring Data Monitoring Without a Schema

This scenario shows how to set an audit configuration to monitor a group of one or more Btrieve data files that have no DDFs. It uses a data file named `sample.btr`, which is installed with a Zen server, as well as an existing audit configuration installed with AuditMaster.

To create your own audit configuration, you must be an AuditMaster administrative user.

A separate example under [Configuring Data Monitoring With a Schema](#) shows how to monitor tables in a database with DDFs.

To use an audit configuration without schemas

1. Start AMCC to open the AuditMaster window, showing the available server.
2. Right-click the server name to select **Login**. You may also simply expand the name to open the login dialog.
3. Enter the default user name **admin** and the password **MASTER**. If you have changed the user name and password, enter those instead.

Note: The built-in user ID **admin** has the default password **MASTER**. Passwords are case-sensitive, but user names are not. This user ID and password are known only within AuditMaster and are unrelated to user accounts under Zen or Windows security.

4. Click **OK**.
5. Under Audit Configurations in the Btrieve Files tab, right-click the existing audit configuration **Zen Generic** and select **Add Group**.
6. Enter a group named **Files**, and click **OK**.

Group names are not case-sensitive and can use any keyboard characters, including spaces, up to 40 characters in length. Although it is possible to reuse a group name from another audit configuration, we recommend a unique name to lessen risk of confusion when you build AuditMaster queries that use group names.

7. In the Btrieve File Group window under the Available Files area, browse to the location of files to monitor. The only files displayed are Btrieve files.

For this example, select the Zen sample directory. In a default Zen installation, this location is `C:\ProgramData\Actian\Zen\samples`.

8. Select the file name **sample.btr**, and click **Select** to move it to the Files to Be Monitored list.

You can also click **Select All** to add every file in the current location.

Each file can be a member of only one group in any audit configuration. If you do not see a file where you expect it to be, check other groups and audit configurations to see if it is already being monitored.

To remove an item from Files to Be Monitored, select it and click **Remove**. Clicking **Remove All** drops all files from the group.

Note: Any query or alert based on a removed file will now fail to find audit records and will also need to be deleted and, if needed, recreated after the file has been added to another group. If the file is added back to the same group as before, the query or alert will again succeed.

9. When you are finished selecting files for the group, click **OK**.

The window closes and AMCC prompts you to restart the Zen database engine.

10. Click **Yes**.

After the restart, monitoring begins. In the Audit Configurations tab, the new group appears with the file listed under it.

11. If you wish to makes changes, right-click the group and select Edit.

Monitoring Items Other than Data Files

One type of Btrieve file other than a data file that you may want to monitor is the Zen server system file dbnames.cfg, found in a default installation under C:\ProgramData\Action\Zen. It is the master list of Zen databases and their configuration settings. You may find it useful to audit it for changes such as new and dropped databases, which appear as inserts and deletes in the dbnames.cfg file. Because dbnames.cfg is a Btrieve file with no schema, its audit records are not human readable. However, they reveal text strings that provide the name and location of the database, as shown in the following example:

101	10/08/2019	01:34:16:120 PM	n/a	Begin Transaction	n/a	<broadcast ops>											
102	10/08/2019	01:34:16:120 PM	dbnames.cfg	Insert	Zen Generic	Files											
103	10/08/2019	01:34:16:400 PM	n/a	End Transaction	n/a	<broadcast ops>											
<																	
Record Details																	
Offset	Data																
	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	[0123456789ABCDEF]
000...	4e	45	57	44	42	20	20	20	20	20	20	20	20	20	20	20	[NEWDB]
000...	20	20	20	20	01	00	00	01	00	00	00	00	00	00	00	00	[bbbbbbbbbbbb]
000...	43	3a	5c	50	52	4f	47	52	41	4d	44	41	54	41	5c	41	[C:\PROGRAMDATA\A]
000...	43	54	49	41	4e	5c	5a	45	4e	5c	4e	45	57	44	42	00	[CTIAN\ZEN\NEWDBp]

Operations to Audit by Table or File

In the Table Group or Btrieve File Group window, each table or file in the group has a list of operations that can be monitored. Clicking a table or file displays the operations monitored for that item. Occurrences of selected operations produce audit records. For example, when the Insert operation is selected, any successful insert into the monitored table or file, regardless of the method of insert, generates an audit record.

In the following example from monitoring the Demodata sample database, the Billing table is selected to show the default selected operations when the table is added to a group.

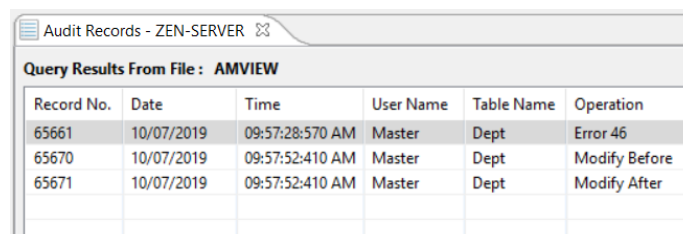


These values can be set for each table or file independently at the time you add it to a group. As with other settings, the Zen database engine must be restarted for changes to take effect.

To change which defaults are offered, see [Operations to Audit Globally](#).

Note that if a selected operation fails, then no audit record is captured. However, AuditMaster also allows you to select certain errors to audit, so that when one of them occurs as part of a failed operation, that error is captured as an audit record.

The following example shows an audit record captured when status code 46 is selected to be audited. The location of the error is the Demodata table Dept, which has been added to a group to be monitored. Status code 46 indicates an invalid owner name, which results here from an attempt to update the table using an incorrect owner name. The update operation produces no audit record because it failed. A second attempt to update the file, this time with a valid owner name, allows the update to succeed, resulting in the Modify Before and Modify After audit records.



Record No.	Date	Time	User Name	Table Name	Operation
65661	10/07/2019	09:57:28:570 AM	Master	Dept	Error 46
65670	10/07/2019	09:57:52:410 AM	Master	Dept	Modify Before
65671	10/07/2019	09:57:52:410 AM	Master	Dept	Modify After

For information about monitoring Zen database status codes, see [Errors to Audit](#).

Querying Audit Records

The following topics describe tasks that involve running queries against the audit records. Before undertaking these tasks, be familiar with the AuditMaster interface, as described in [Using AuditMaster Control Center](#).

- [Displaying Audit Records](#)
- [Running Queries](#)
- [Working with Archived Audit Records](#)
- [Working with Alerts](#)
- [Searching Audit or Log Records](#)
- [Exporting Audit or Log Records to a Text File](#)
- [Displaying Audit Records under Zen Security](#)
- [Using AuditMaster Undo](#)

Displaying Audit Records

AuditMaster monitors a Zen database engine for operations on Btrieve files, logs those events, and captures data from the records involved. It stores all of these things in a log file designed to receive large amounts of information. To enable you to access its contents, data is copied from the log file to a view file and prepared for running queries. As the view file grows, its query performance may slow. To remedy this, its contents can be moved to archives.

To display audit data, you run a query. AMCC offers two types of queries: regular and advanced. Regular queries use attributes of audit records to return a table of results. Advanced queries can also query for values in the database records captured with the audit records.

The following topics provide a quick introduction to working with audit records.


- [Running a Regular Query on the View File](#)
- [Working with the Audit Records Tab](#)
- [Reviewing Audit Data Columns](#)
- [Viewing Audit Record Details](#)

Running a Regular Query on the View File

This basic example shows the simplest way to display audit records.

To update the current view file

Before you query the view file, you update it first to retrieve the latest audit records from the log file.


1. In the data tree, right-click the current view file and select **Update Current View File**, or in the toolbar click the icon .

You may now query the view file for audit records.

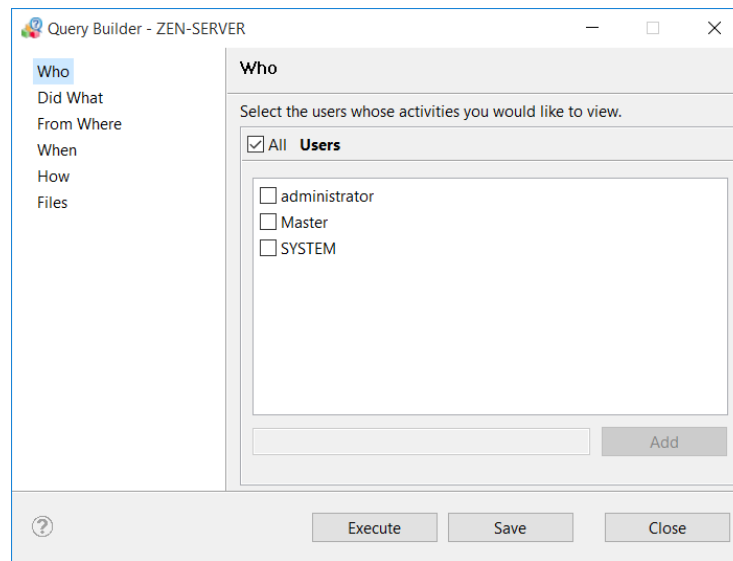
2. If you would like to check the number of records in the view file and their first and last dates of capture, right-click the current view file and select **Properties**.

To run a default regular query

1. Click the current view file in the data tree.
2. Do any of the following to open the Query Builder window:
 - Double-click the view file.

- Right-click the file and select **Query**.
- Select the file and then the **File > Query** command.
- Select the file and then in the toolbar, select the new query icon .
- Press **Alt-Q**.

The Query Builder window opens to display the first of six groups of search conditions that you can use to restrict the query. The options shown are based on values found in the current view or archive file being queried.



For each group of search conditions, all options are selected by default except for the following:

- Under Did What, only Zen database operations and selected Zen status code messages are selected for the query. AuditMaster internal and debug messages are not selected.
- Under Files, the file checked is the one selected before the Query Builder window was opened. Any other file needed for the query must be manually added.

Selecting all options means that the query result returns every record in the view file for display in the Audit Records tab. For details about using the search conditions to restrict queries, see [Running Queries](#).

3. Click the **Execute** button.

The query result appears in the Audit Records tab. The Query Builder window remains open and can be moved to view the result.

Record N...	Date	Time	Machine Name	User Name	Table Name	Operation
264	09/19/2019	02:44:59:740 PM	Zen-Server.englab.local	Master	Student	Insert
225	09/19/2019	01:21:52:510 PM	Zen-Server.englab.local	Master	Student	Modify Before
226	09/19/2019	01:21:52:510 PM	Zen-Server.englab.local	Master	Student	Modify After
221	09/19/2019	01:21:33:810 PM	Zen-Server.englab.local	Master	Student	Modify Before
222	09/19/2019	01:21:33:810 PM	Zen-Server.englab.local	Master	Student	Modify After
208	09/19/2019	01:19:44:270 PM	Zen-Server.englab.local	Master	Student	Insert
204	09/19/2019	01:15:58:370 PM	Zen-Server.englab.local	Master	Student	Modify Before
205	09/19/2019	01:15:58:370 PM	Zen-Server.englab.local	Master	Student	Modify After

4. You can now do several things:

- Change which columns are displayed and the order in which they appear. See [Working with the Audit Records Tab](#).
- View individual record detail. See [Viewing Audit Record Details](#).
- Adjust the query and execute it again, as described under [Running Queries](#).
- Save the query by clicking **Save**. See [Running a Saved Query or Last Query Executed](#).
- When you are done querying, click the **Close** button in the Query Builder window.


Working with the Audit Records Tab

The Audit Records tab displays the results of a query. The columns in the tab show capture date and time, table name, operation, user name, and other audit information. The following table provides options for customizing and working with the display.

Option	Steps
Set columns to display	See Reviewing Audit Data Columns , which also describes column contents.
Adjust column widths	Click and drag the edge of a column to the desired width.
Change column order	Drag a column to the desired position.
Sort record order	Click the heading of a column to sort rows in ascending or descending order based on the values in that column. To return to the original sort order, close the tab and rerun the query.
Save these column settings	Select View > Preferences > Table Layout and click check boxes for each setting.
Search audit records	See To search audit or log records .

Option	Steps
Export audit records	See To export audit records .

Reviewing Audit Data Columns

The following table lists all possible audit data columns. You can choose the ones to display by clicking the Select Columns to Display icon  above the tab. Column order can be rearranged by dragging columns with the mouse. If you would like to save and reuse these settings, select **View > Preferences > Table Layout**.

Column Name	Contents
Record No.	Incremental unique number for audit record
Dependent Record	Record number for earlier related record: <ul style="list-style-type: none"> • Modify-before record for modify-after record • Begin-transaction record for end/abort transaction record
Date	Capture date for audit record
Time	Capture time for audit record
Machine Name	Machine name or IP address where the event originated.
User Name	Login ID under which event occurred. See Displaying Audit Records under Zen Security .
Database Name	Database in which event occurred. See Displaying Audit Records under Zen Security .
Table Name	Table or data file in which event occurred. The table or file must be listed for monitoring in an audit configuration. All monitored files appear in the Tables list of the Did What tab in Query Builder.
Operation	Database event. Events can include any item in the Operations list of the Did What tab in Query Builder. SQL logins appear in this column. Selected Zen status codes also appear here when first selected in the Errors to Audit section of the Server Settings window. For details see Maintaining Server Settings .
Operation Context	BTRIEVE is the context for all data file operations.
Database Engine	Either AM Message API (internal use within AuditMaster) or Zen
Database Version	Version of Zen running on server
Product	As listed in audit configuration for monitored file
Product Version	As listed in audit configuration for monitored file

Column Name	Contents
Group Name	Group for monitored file in audit configuration
Component	As listed in audit configuration for monitored file
Component Version	As listed in audit configuration for monitored file
Process Name	Process that was the source of the operation. Typically, most of these are Zen Engine, with a few actions done by AuditMaster, which are listed as Zen Monitor.
OS Version	Name and version of operating system of system where AuditMaster server is running
View File	Location of audit record, either amview (current view file) or the archive file name

Viewing Audit Record Details

To see the detail of an individual audit record, click the record in the Audit Records tab to display it in the lower part of the AMCC window. If the audit record captures changes to an application data record, both before and after values are shown and highlighted in red.

If the database schema has been imported, then the changes are readable, as in the following Demodata example. If no schema is used, then the changes are shown in hexadecimal.

Record Details		
Field Name	Before	After
ID	175828156	175828156
Cumulative_GPA	3.450	3.450
Tuition_ID	6	6
Transfer_Credits	30	30
Major	Computer Science	Computer Science
Minor	Math	Math
Scholarship_Amount	1800.00	1800.00
Cumulative_Hours	44	56

Running Queries

To display audit records from a current view or archive file, you must run a query. By default, the query returns all available audit records associated with tables or data files monitored in audit configurations. You can restrict the query using search conditions for [Who](#), [Did What](#), [From Where](#), [When](#), [How](#), and [Files](#). For example, you can search for audited events on a particular date, for events from a selected table, or for changes that were made by only one user.

This topic covers the following tasks:

- [Displaying All Audit Records](#)
- [Restricting a Query](#)
- [Building an Advanced Query](#)
- [Using the Files Group in Queries](#)
- [Running a Saved Query or Last Query Executed](#)

Displaying All Audit Records

The simplest query in the Query Builder window is the default, which displays all audit records in the current view file.

To display all available audit records

1. Right-click the view file and select **Update Current View File**.
2. Select the view file and select **File > Query**, or right-click and select **Query**.
3. In the Query Builder window, by default all options are selected for each search condition. To display all AuditMaster data for this file, simply select **Execute**.

Audit records are displayed in the grid in the upper right-hand pane of AMCC.

Instead of selecting the view file, you can select or right-click an archive file. If you want to select more than one archive file, or if you want to select both the view file and one or more archive files, see [Files](#).

Restricting a Query

Query Builder provides sets of search conditions for restricting a query to who, did what, from where, when, how, and in which files of audit records to search.

To restrict a query

1. In Query Builder you can select options to make a query more selective. These search conditions are on the left and are described in the following table.

To find...	Use Option...	Perform these steps...
Users For events that involve specific Zen, Windows, or AuditMaster users, as shown in the User Name column	Who	<ol style="list-style-type: none">1. To find audit records involving specific users, clear the All Users check box.2. In the list of users, select users by checking the box beside their name. The users listed are those found in the view or archive file to be queried. <p>You can add a user by entering a login name and clicking Add.</p>
Operations, Groups, and Tables For audit records from selected operations, in selected tables, in selected groups, as shown in the Operation, Group Name, and Table Name columns	Did What	<ol style="list-style-type: none">1. To find a type of operation, such as insert or delete, clear the All Operations check box. You can also clear All Groups or All Tables to make their lists available.2. Select the operations and any items affected by them. Expand lists as needed to select the appropriate options. Use the Shift or Ctrl keys to extend the selection. You may select tables and files regardless of their audit configuration or group. You can also combine files with or without schemas in the same query. <p>Note: After clearing the All check box, when you expand a node you may still see all items selected. To remove the selection, click a single item in the list.</p>
Machines For audit records captured on selected machines, as shown in the Machine Name column	From Where	<ol style="list-style-type: none">1. To find a machine, clear the All Machines check box. The list of machine names and network addresses is now available.2. Select one or more machines by clicking a check box. If needed, you can add a name or network address by entering it and clicking Add.

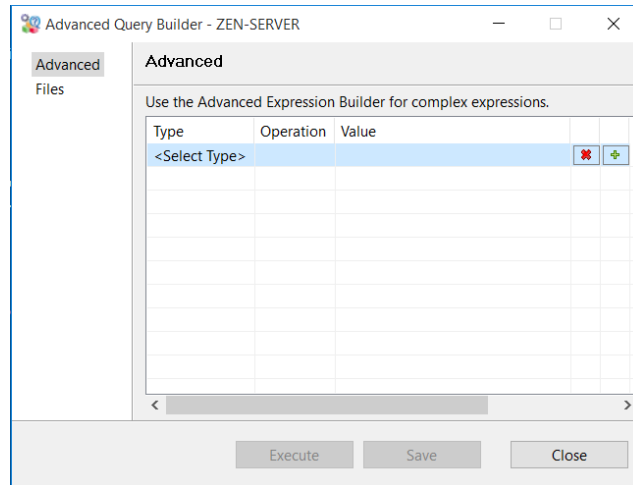
To find...	Use Option...	Perform these steps...
Specific Dates For audit records captured on certain dates, within a time range for each day selected, in the Date and Time columns	When	<ol style="list-style-type: none"> 1. To search within a start and end date, clear the All Date Range check box to see Start Date and End Date calendars. 2. Select a day, month, and year from the calendars or enter the date and click Set. 3. To search within a time range for each day in the date range, clear the Time Range option. Select a time from the Start Time and End Time fields. You can enter a time directly. <p>Note: The time range applies to each individual day in the date range – for example, between 8:00 a.m. and 5:00 p.m. each day. If All Time Range is reselected, it returns to the default of 24 hours, but the manually entered times remain and can be reactivated by clearing All Time Range again. The same is true if you set a date range and then reselect All Date Range.</p>
Processes or Programs For audit records logged for certain processes or programs, in the Process Name column	How	<ol style="list-style-type: none"> 1. To find a specific process or program, clear the All Processes option. The processes are now available. 2. Select a program or process by clicking the box beside the option. If the process name does not appear, use the Add field at the bottom of the pane to include it in the list.
Audit Record Files For audit records returned from selected view or archive files, as shown in the View File column	Files	<ol style="list-style-type: none"> 1. The current view file is selected by default. You can leave it selected or clear it to exclude it from the query. 2. You can select an archive file by clicking its check box. <p>Note: If an archive file is not visible, it may be compressed. Close the Query Builder, decompress it, and then create your query.</p>

2. At any time while making your selections, you can run the current query by clicking **Execute**.
3. Review the result in the Audit Records tab. If it is not what you need, return to Query Builder, make adjustments, and then run the query again.
4. When you are satisfied with the query, if you would like to reuse it later, click **Save**.

In the Save Query dialog box, enter a descriptive name for the query. You can use up to 60 characters, including spaces. Then click **OK**. The name can be changed later, if needed. For more information on using a saved query, see [Running a Saved Query or Last Query Executed](#).

Building an Advanced Query

Advanced Query Builder can create more complex queries than Query Builder. It uses expressions to search audit records for specific events. If the schema has been imported, it can also query the contents of fields in data records captured with auditing data.



The Select Type and Operator columns offer the following elements for building a query expression. All text values entered are case-sensitive. The phrase “same as” refers to comparable search options in the regular Query Builder window.

Attribute	Description
(Open parenthesis to build an expression block
Data Field	Same as selecting a table under Did What, except that you can further restrict the query at the column level and enter a value to search for or compare
Date	Same as Date Range attribute in When tab
Group	Same as Groups attribute in Did What in regular
Database Name	The name of the audit configuration where a schema was imported, rather than the name of the database itself. For Btrieve files, which have no schema, the Zen internal database DefaultDB is used.
Table	Same as Table attribute in Did What tab
Operation	Same as Operations attribute in Did What tab
How	Same as Process attribute in How tab
Rec ID	Record number in Audit Records tab of the query result
Time	Same as Time Range attribute in When tab

Attribute	Description
Where	Same as Machine Name attribute in From Where tab
Who	Same as User attribute in Who tab
and, or	Logical operators used in the Type column
=, >, >=, <=, <, in	Comparison operators used in the Operator column, plus “in” as a set operator for a list of elements
)	Close parenthesis to build an expression block

Advanced Query Examples

This topic offers two tutorials to show how to build complex queries:

- [To query for audit records of students with GPA 3.0 or greater](#)
- [To find the date and time for the insert of a particular student](#)

The first query searches for all audit records where the cumulative GPA of a student is 3.0 or greater. The second one modifies the first one to find the date and time when the insert of a specific student occurred.

To follow the tutorials, you must first do three things:

- In AMCC, under the built-in Zen Demo audit configuration, create a group called Demo, add all Demodata tables to the group to begin auditing them, and restart Zen engine services.
- To make changes in one of the monitored tables, in ZenCC open a SQL document set to the Demodata database context and run this SQL script:

```
INSERT INTO Student(ID, Cumulative_GPA, Tuition_ID, Transfer_Credits, Major, Minor,
Scholarship_Amount, Cumulative_Hours) VALUES (213725554, 3.6, 6, 30, 'Biology', 'Technical
Writing', 2600.00, 24);
UPDATE Student SET Cumulative_GPA = 3.1 WHERE ID = 189602671;
UPDATE Student SET Cumulative_GPA = 3.5 WHERE ID = 189152021;
```

- In AMCC, right-click the current view file in the data tree and select **Update Current View File** so that AuditMaster can query the latest contents of the view file and archive files.

To query for audit records of students with GPA 3.0 or greater

1. Do any of the following to open the Advanced Query Builder window:
 - Right-click the view file and select **Advanced Query**.
 - Select the file and then select **File > Advanced Query**.
 - Select the file and then press **Ctrl-Alt-Q**.

In this window, the Advanced group of query options is selected by default and is used here. The Files group is explained under [Using the Files Group in Queries](#).

2. In the Type column, click **<Select Type>**.
3. In the list of query attribute types, select **Data Field**.
4. For Data Field Selection, expand **Zen Demo > User Tables > Student** and select **Cumulative_GPA**.
5. In the value field at the bottom, enter **3.0** and click **OK**.
6. For the Data Field operator, select **>=** for greater than or equal to 3.0.

The Advanced Query Builder window should now look like this:

Type	Operat...	Value
Data Field	>=	Zen Demo (9)\<User Tables>\Student\Cumulative_GPA = 3.0
<Select Typ...		

The query is now set to search for all audit records of changes in the Student table for students who have a GPA of 3.0 or greater.

7. Click **Execute**. Leave the window open, but move it if needed to see the AMCC window.

The query result is displayed in the Audit Records tab and should include the newly inserted and modified rows:

Audit Records - ZEN-SERVER

Status Log - ZEN-SERVER

Query Results From File : AMVIEW

Record No.	Date	Time	Table Name	Operation
109	10/02/2019	11:38:24:800 A...	Student	Insert
113	10/02/2019	05:05:07:650 PM	Student	Modify After
117	10/02/2019	05:06:46:720 PM	Student	Modify After

Note the following things:

- The query returns these audit records because changes have occurred in their records in Demodata since auditing began on the Student table, which AuditMaster captured and which were in the current view file.
- Although Demodata contains existing records of other students with GPAs 3.0 or greater, no changes to those records have occurred, so AuditMaster has no audit records of them and AM queries return no results for them.

To find the date and time for the insert of a particular student

In the last step of the first tutorial, you left the Advanced Query Builder window open. This second tutorial continues in that window.

1. In the query window, click the value for the Data Field, which is currently **Zen Demo (9)\<User Tables>\Student\Cumulative_GPA=3.0**.
2. Click the **ellipsis button** that appears to the right of the entry.
3. In the Data Field Selection window, change the selected data field by expanding **Zen Demo > User Tables > Student** and selecting **ID** to replace **Cumulative_GPA**.
4. For the ID value, enter **213725554**, the number of the student in the record inserted earlier, and click **OK**.
5. For the Data Field operator, select **=** for equal to the student ID number.
6. For this example, let us imagine that you know the student must have been added in the current month, but you would like to know exactly when this happened. Click **<Select Type>** and select **and** to extend the query.
7. Click **<Select Type>** and select **Operation**.
8. For Operation Selection, expand **ACTIAN ZEN** and select **Insert**.
9. Click **<Select Type>** and select **and** to extend the query.
10. Click **<Select Type>** and select **Date**.
11. Select the **first day** of the current month and click **OK**.
12. In the line just created, for the Data Field operator select **>=** for greater than or equal to the first selected date.
13. Click **<Select Type>** and select **and** to continue the date range.
14. Click **<Select Type>**, select **Date**, select the **last day** of the current month, and click **OK**.
15. In this new line, for Data Field operator select **<=** for less than or equal to the second selected date.

The Advanced Query Builder window should now look like this:

Type	Operat...	Value
Data Field	=	Zen Demo (9)\<User Tables>\Student\ID = 213725554
and		
Operation	in	ACTIAN ZEN\Insert
and		
Date	>=	10/01/2019
and		
Date	<=	10/31/2019
<Select Typ...		

16. Click **Execute** to run the query.

The query result is displayed in the Audit Records tab and looks like this:

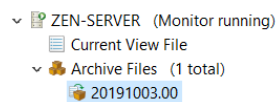
Audit Records - ZEN-SERVER				
Status Log - ZEN-SERVER				
Query Results From File : AMVIEW				
Record No.	Date	Time	Table Name	Operation
109	10/02/2019	11:38:24:800 A...	Student	Insert
< [Progress Bar]				
Record Details				
Field Name		Field Value		
ID		213725554		
Cumulative_GPA		3.600		
Tuition_ID		3		
Transfer_Credits		30		
Major		Biology		
Minor		Technical Writing		
Scholarship_Amount		2600.00		
Cumulative_Hours		24		

Using the Files Group in Queries

In the Advanced Query Builder window, the Files group allows you to select the current view and any uncompressed archive files you would like to include in a query. You can also select only archive files.

To follow this tutorial, you must have done the following steps:

- In AMCC under Audit Servers, right-click **Current View File** and select **Archive**.
- Expand the Archive Files node in the data tree to see the name of the new file, which is named based on the archive date, which should resemble the following:



To select files to include in a query

1. In the Advanced Query Builder window, click **Files**. The Current View File option is selected by default.

Files				
Select the files to be queried.				
File Name	Start Date	End Date	No Reco...	
<input checked="" type="checkbox"/> Current View File	10/03/2019	10/03/2019	12	
<input type="checkbox"/> 20191003.00	09/30/2019	10/03/2019	131	

If you left only the default view file selected and ran either of the queries from the two previous Advanced Query Builder tutorials, no results would be returned. When you archived the view file, all of its audit records were moved to the new archive file.

2. To run a query against both the archive file, select it instead of Current View File. Or select them both.

Since you can query only uncompressed audit records, compressed archive files are not listed under the Files group. To see a file that is not listed, you must decompress it. For more information, see [Working with Archived Audit Records](#).

Running a Saved Query or Last Query Executed

For each AuditMaster server, queries previously saved are stored in the data tree under Saved Queries. In addition, the last query executed is always saved and can be resubmitted. This section covers the following topics:

- [To save a query](#)
- [To use a saved query](#)
- [To use the last query executed](#)

To save a query

1. After creating a query in either Query Builder or Advanced Query Builder, click the **Save** button to name the query.
2. Enter a descriptive query name and click **Save**. You can leave the query builder window open.

The saved query appears with the name you gave it in the Audit Servers data tree.

To use a saved query

1. If needed, to update the data tree, right-click the Saved Queries node and select **Refresh**.
2. Expand the **Saved Queries** node.
3. Right-click a query to see a list of commands:
 - **Query Current View File**. Run the query against the current view file.
 - **Query Multiple View Files**. Display available files to select the ones needed and run the query.

-
- **Rename.** Change the name of the query. You can use up to 60 characters, including spaces.
 - **Delete.** Remove the query permanently.

Only uncompressed audit records can be queried. If a file used in a query has been compressed, you must decompress it to run the query.

Note: The larger the compressed file, the longer it takes to decompress. To be sure that all records are ready to query, right-click the Archive Files node and select **Refresh** to update the display. When ready, the archive file icon changes from a small box in a vice to an arrow pointing to a bigger box.

To use the last query executed

In the data tree, right-click the view file or an archive file and select **Execute Last Query**.

Working with Archived Audit Records

Auditing can generate large numbers of audit records. As the size of the current view file rises, queries against it can take longer to run. To improve performance, AuditMaster provides the ability to move audit records from the current view file to an archive file. Archiving can be done automatically or manually. In automatic archiving, AuditMaster creates an archive file when the current view file reaches a set limit by size or by date and time. Manual archiving must be done by a user with administrative permissions.

Archive files appear in the data tree with a file name that uses creation time in the format *yyyymmdd.nn*, where *yyyy* is the year, *mm* is the month, *dd* is the day, and *nn* is the number of the archive file created that day, from 00 to 99.

Compressing archive files saves as much as 90 percent disk space. AuditMaster encrypts compressed archive files to restrict access to only users within the AuditMaster system.

The following topics provide more detail on the use of archive files:

- [Manual Archiving](#)
- [Managing Archives](#)
- [Automatic Archiving](#)

Manual Archiving

This topic gives steps for two tasks:

- [To archive manually](#)
- [To set the number of archive files shown](#)

To archive manually

You may want to archive manually for the following reasons:

- The audit log has grown large, queries and other operations take longer, and you do not want to wait until the next automated archiving to regain performance speed.
- Automated archiving will not occur soon, but an event of interest makes it preferable to archive now.
- You wish to archive and compress records to manage disk space.

In the data tree, right-click the current view file and do one of two things:

- Select **Archive**.

- Select **Archive and Compress**. Large numbers of records can take time, so you may want to check the Status Log tab for the “Finished compressing” message. If needed, refresh the log to see the latest entries.

You cannot run a query against a compressed archive file. You must first decompress it by right-clicking and selecting **Decompress**.

Note: In the data tree, you may sometimes need to right-click the Archive Files icon and select **Refresh** to update the list.

To set the number of archive files shown

You can control the maximum number of uncompressed and compressed archive files shown in the data tree. The list displayed is the same whether the files were created manually or automatically. To open this setting, select **View > Preferences > Archives**.

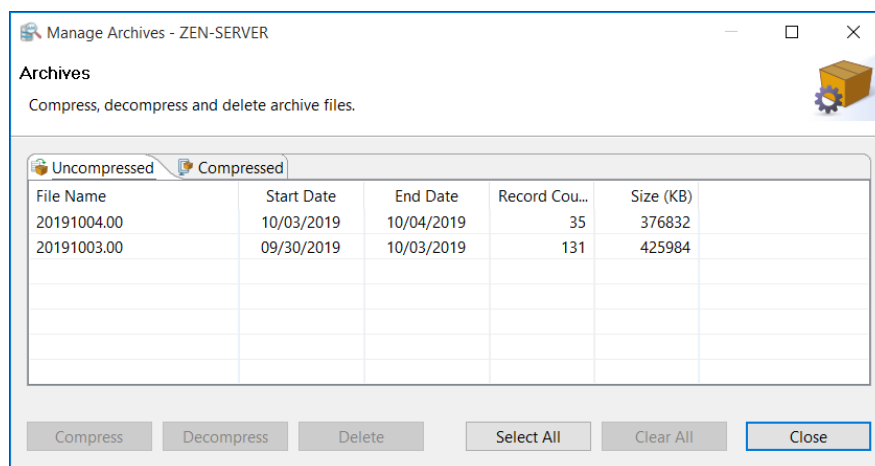
The default setting is 30. Displaying a list shorter than the available number of files does not delete them but simply removes them from the display. Raising the number in the setting displays them again.

After changing this setting, you may need to right-click the Archive Files icon and select **Refresh**.

Changing this setting does not affect the display of archive files in the Manage Archives window, described in [Managing Archives](#).

Managing Archives

In the data tree, you select only one archive file at a time. The Manage Archives window lets you work with archive files as a group. You can open it by selecting **Tools > Manage Archives**.



To use the window, select an archive file and use the buttons to compress, decompress, or delete it. Use the Shift or Ctrl keys to select more than one file.

Working with Alerts

AuditMaster provides an alert capability for real-time detection of a particular audit event defined by a query. When an event matching the query occurs, AuditMaster does two things:

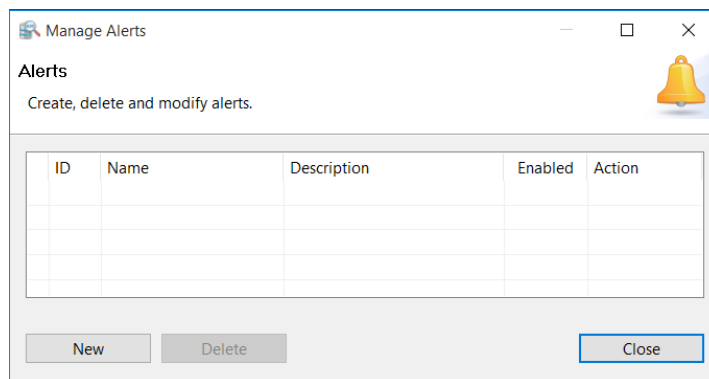
- It flags each audit record in the alert query result with a bell icon 🔔. The bell flag becomes a permanent part of the audit record and appears in any query result that contains the record.
- It writes an entry to the Windows Application event log. This logging provides network administrators the ability to use tools for running automatic programs or sending notifications.

To create an alert

1. In AMCC, create and save a query for the type of audit records that the alert is to detect.

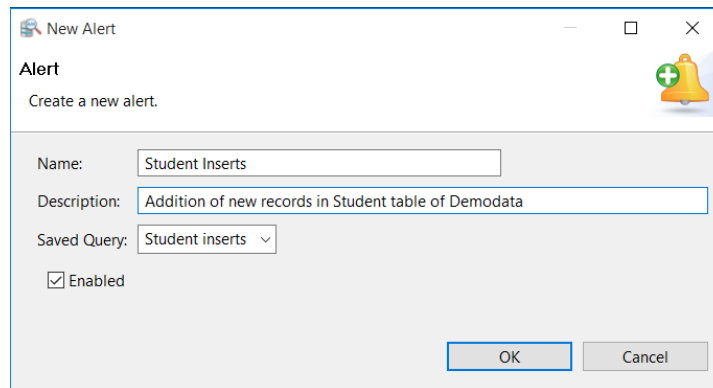
Note: The saved query used to create the alert must have at least one restriction. In other words, it cannot be equivalent to `SELECT *`. At least one search condition in the alert query must be set.

2. Select **Admin > Manage Alerts** to open the Manage Alerts window.



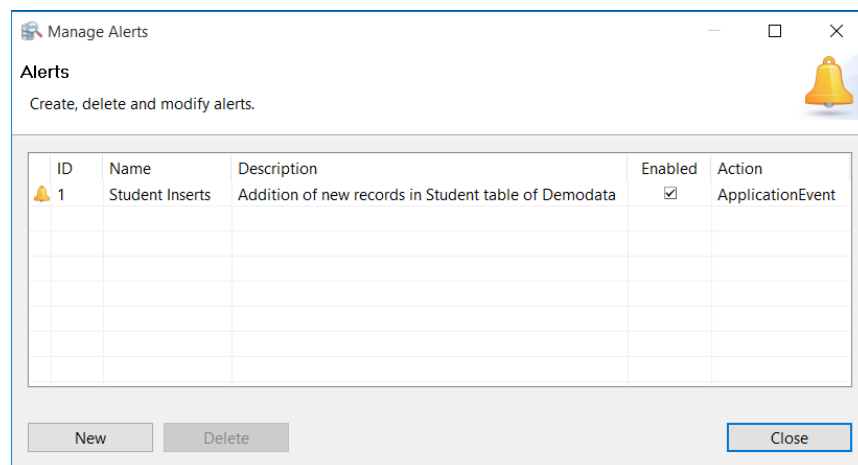
3. Click **New** to open a New Alert window.
4. Enter a name for this alert, using letters, numbers, or spaces up to 40 characters.
In this example, we create an alert for new students in the Demodata database.

5. Enter a description for the alert, using up to 100 characters.



The 'New Alert' dialog box is shown. It has a title bar with a bell icon and standard window controls. The main area is titled 'Alert' with the instruction 'Create a new alert.' Below this, there are three input fields: 'Name' with the text 'Student Inserts', 'Description' with the text 'Addition of new records in Student table of Demodata', and 'Saved Query' with a dropdown menu showing 'Student inserts'. There is a checked checkbox labeled 'Enabled'. At the bottom right are 'OK' and 'Cancel' buttons.

6. In the Saved Query list, select the query to be used.
7. Click **OK** to return to the Manage Alerts window, which shows the added alert.



The 'Manage Alerts' window is shown. It has a title bar with a bell icon and standard window controls. The main area is titled 'Alerts' with the instruction 'Create, delete and modify alerts.' Below this is a table with the following data:

ID	Name	Description	Enabled	Action
1	Student Inserts	Addition of new records in Student table of Demodata	<input checked="" type="checkbox"/>	ApplicationEvent

At the bottom are 'New', 'Delete', and 'Close' buttons.

After the Zen database service restarts, the alert becomes active. Database activity triggers an alert when any audit record is captured that matches the selected saved query. The audit record is flagged with a bell icon 🛎 that appears in any query result containing that audit record.

In addition to flagging the audit record, AuditMaster writes an entry to the Windows Application log in %SystemRoot%\System32\Winevt\Logs\Application.evtx. When displayed in Windows Event Viewer, the log entry resembles the following:

Level	Date and Time	Source	Event ID	Task Category
Information	10/7/2019 5:00:07 PM	Action AuditMaster	16717	AuditMaster Alert

Note: When you use Windows Event Viewer to see logged alerts, it may be helpful to open Filter Current Log and set the event source to Actian AuditMaster.

As shown in the following information for this event log entry, the data detail from the Zen database record is the same as that shown for the audit record in AMCC:

```
Alert 'Student Inserts' Fired on Record ID: 55
Alert ID: 1
Desc: Addition of new records in Student table of Demodata
```

Audit Information

=====

```
Rec Id:      55
Date:        07/10/2019
Time:        17:00:07
DBMS:        Actian Zen
DB Ver:      14.0.41
Op Context:  BTRIEVE
Operation:   Insert
Dep Rec Id:  0
Product:     Zen Demo
Product Ver: 9
Component:   <User Tables>
Component Ver: 9
Table:       Student
Group:       Demo
Net Address: Zen-Server.englab.local
Net User ID: Master
Process:     Zen Engine
Monitor Ver: Zen Demo
OS Ver:      W2K 6.2.9200
Return Code: 0
```

Record Data

=====

```
ID:          334651124
Cumulative_GPA: 3.400
Tuition_ID:   5
Transfer_Credits: 12
Major:        Computer Science
Minor:        Statistics
Scholarship_Amount: 0.00
Cumulative_Hours: 12
```

Additional Information

=====

```
View Path:    \\ZEN-SERVER\PVSWAUDIT$\data\
Server Net ID: 192.168.149.142
```

Audit Alert Best Practices

In using alerts, consider the following:

- Selecting the Enabled check box activates the alert. Clearing the check box deactivates it, meaning that no audit record matching the query can trigger an alert. As a result, no bell icons

will be shown for these audit records in any query result, and no entry will be written to the Windows event log.


- Dramatic and undesirable logging may arise from an alert with a broad query that is likely to match a large number of audit records. It is best practice to narrow the query to only useful information that requires additional action.
- In a similar way, if you are expecting bulk loading of a large number of data records whose audit logging will lead to alert query matches, then it may be helpful to disable those alerts before the bulk load and then reenable them afterward.

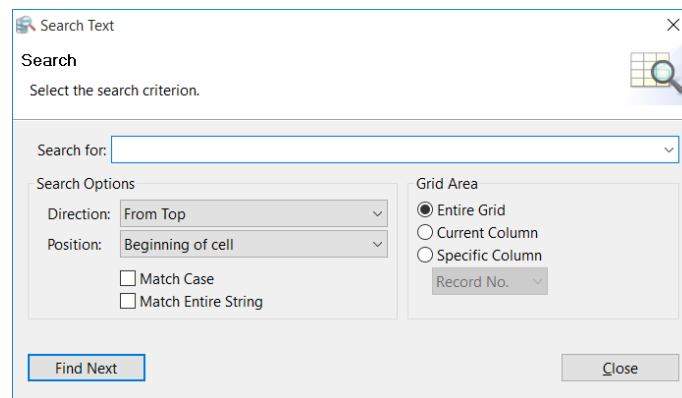
Searching Audit or Log Records

You can use the search command to find particular strings such as users, dates, times, and other values in the Audit Records tab or the Status log tab. The search feature provides a number of options, including case-sensitivity and restriction to certain tab columns.

Note: Depending on the number of records and the complexity of the search criteria, it may take some time to complete your search. Whenever possible, try to narrow your criteria.

To search audit or log records

1. Select the Audit Records or Status Log tab. Refresh the entries shown, if needed.
2. Select **Tools > Search** or click the **Search icon**  to the right above the tab.



3. In the Search For field, enter a text string to find in the currently displayed audit records.
4. If needed, use the Search Options to narrow your search.
 - In the Direction options, select a direction to start the search. These include, **From Top** row down, the **Next** row down, and the **Previous** row down.
 - In the Position options, select a search position. Select **Beginning of cell** or **Anywhere**.
 - To match upper and lower case spellings, select the **Match Case** check box.
 - To match the entire search string instead of just part, select the **Match Entire String** check box.
5. If needed, use the Grid Area to narrow your search.
 - Select **Entire Grid** to search all columns.
 - Select **Current Column** to search only the column highlighted by the current match.
 - Select **Specific Column** and choose a column name from the list.

6. Click **Find Next**.


If a matching string is found, it is highlighted in the tab. The Search Text window also displays its location in the query result. Continue clicking Find Next to see more matches. Once you reach the last match, clicking Find Next again displays the message “No match found.” If you want to return to an earlier match, close the Search Text window and reopen it to search again. The string you entered is saved from the last search.

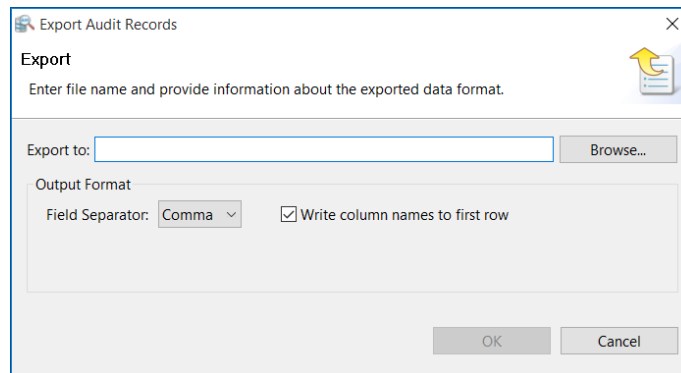
Exporting Audit or Log Records to a Text File

AuditMaster can export the displayed contents of the Audit Records or Status Log tab to a comma- or tab-delimited text file.

Only records and columns displayed in the tab are exported. You can use the Select Columns to Display setting to change which columns are included in the exported text.

To export audit records

1. Select the Audit Records or Status Log tab. For the Audit Records tab, refresh the current view file and rerun the query, if needed.
2. Select **Tools > Export** or click the **Export icon**  to the right above the tab.



3. In the Export window, click the Browse button to select a path name for the exported file. The default location is C:\Users\<user name>\<file name>. Add a file name suffix such as .txt if needed.
4. For the field separator, select comma or tab.
5. Choose whether to use the default option to write column names to the first row of the exported file.
6. Click **OK** to export the file.

Displaying Audit Records under Zen Security

If you run AuditMaster with Zen security enabled, field values in the User Name and Database Name columns vary with DefaultDB database security policy and type of database operation, as shown in the following table.

Security Policy	Btrieve Operations		SQL Engine Operations	
	User Name Displayed	Database Name Displayed	User Name Displayed	Database Name Displayed
Database	Database login	One of the following:	Database login	n/a
Mixed	Database login	<ul style="list-style-type: none">Database name from Btrieve Login API or connection string	Database login	n/a
Classic	<ul style="list-style-type: none">OS loginDatabase user name if database security enabled	<ul style="list-style-type: none">Database name bound to Btrieve file on which operation executed, if anyDefaultDB if other two unavailable	<ul style="list-style-type: none">OS loginDatabase user name if database security enabled	n/a

Audited Btrieve operations include Select/Read, Insert, Update, Delete, Login, and Logout. For Begin Transaction, End Transaction, Abort Transaction, and Reset operations, which are not associated with a specific database, the database name is not available.

Login errors are listed with the invalid user name and database name when available. For SQL logins, the host name is not known at login time but becomes available afterward and is displayed for SQL operations.

Under Mixed security, database logins match operating system or network logins.

For more information on the relationship of AuditMaster logins to Windows and Zen database logins, see [Running AuditMaster under Zen Security](#). For more information on database operations in a Zen security environment, see *Advanced Operations Guide*.

Using AuditMaster Undo

The AuditMaster Undo command makes it possible to reverse certain database events. A successful undo depends on the operation and the current state of the record involved, which may have changed again since the capture of the audit event you are reviewing. For example, in the case of an update to a data field, the Before value in the audit record Modify Before and Modify After detail shows the data that AuditMaster can attempt to restore.

Operation	Results of Undo
Insert	Deletes record, if it still exists and no other conditions stop insertion
Delete	Reinserts record if it does not exist, or if it does, so long as duplicates are allowed and no other conditions prohibit the insertion
Update	Restores Before state of record, if it still exists and no other conditions stop the update

Caution! Before attempting an undo, consider the following:

- The Windows user name under which you log in and run AMCC must have write permission for the Zen database being monitored. Neither Windows nor the Zen server recognize the AuditMaster administrator and regular user accounts created within AuditMaster.
- The file listed in the audit record must not have been removed from its audit configuration group since the operation occurred.
- Undoing operations from within AuditMaster carries a risk of putting application data into an inconsistent or illogical state. You should be an advanced Zen user who understands the cautions regarding changing one part of an application database independently of another part.
- If files in an audit configuration group have the same name but different paths, undo applies only to the first file listed.

Note: Remote client logins do not support undo.

To undo a database operation

1. In the Audit Records tab, right-click an audit record and select **Undo Operation**. Undo is available only for certain operations, such as Insert, Delete, or Modify Before/After.
2. When prompted to confirm the undo attempt, click **Yes**, or **No** if you change your mind.

Note: Each undo operation is captured by AuditMaster and can also be reversed by an undo.

Administering AuditMaster

As an administrator, you will perform certain tasks to define how AuditMaster operates. As for adding audit configurations, the menu commands for these tasks are available only to users with administrative rights.

- [Adding and Removing Servers](#)
- [Reviewing Activity in the Status Log](#)
- [Disabling and Enabling the Monitor](#)
- [Maintaining Users](#)
- [Maintaining Server Settings](#)
- [Replacing the Network Share with a Local Path](#)

Adding and Removing Servers

An audit server is a Zen server where AuditMaster is installed. The file **amserver** contains audit server connection settings. In a default installation, it is found in C:\ProgramData\Actian\Zen\Audit\DATA.

- [Adding a Server](#)
- [Removing a Server](#)

Adding a Server

In an AuditMaster installation, the local Zen server is automatically added as an audit server. You can manually add a remote audit server if you have network access and file system permissions under your Windows login.

To add a server

1. Check the server that you wish to add to make sure that the Zen database engine is running.
2. In AMCC, select **Server > Add**.
3. Enter the path to the **amserver** file for the audit server.

In a default installation, this path is \\server\PVSWAUDIT\$\DATA\amserver, where *server* is the name of the Zen database server. Note that a custom share name may not be PVSWAUDIT\$.

4. Click **OK**.

The server you selected is added to the data tree.

Depending on your system and network, the added name may be the machine name or the path to the amserver file.

Note: If your client cannot connect successfully to the AuditMaster server, you may receive a – 108 error message. The cause may be a faulty network mapping or other network problem. It may also involve a license key with too low a user count. See [Authorization License](#).

5. Expand the new audit server to log in, or right-click it and select Login.
6. In the login dialog, enter an AuditMaster user name and password, and click **OK**.

The remote audit server is now ready for use.

Removing a Server

When you remove an audit server connection from an AMCC data tree, the client no longer has access to that server. However, auditing continues on the server, and existing audit records, users, and settings remain because the Zen server is where they are stored. If you add the server connection again, everything that was present before is again displayed in the data tree.

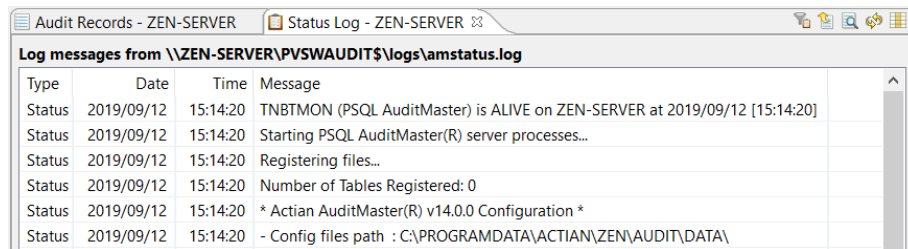
To remove a server

1. Click an audit server in the data tree and select **Server > Remove**.
2. In the dialog box, select **Yes** to confirm.

Reviewing Activity in the Status Log






The Status Log tab displays logging that AuditMaster performs on itself. The tab provides a list of status and error messages generated by AuditMaster operations. For developers, it also can be configured to capture messages for debugging purposes.

You can open the Status Log tab by selecting **Admin > View Status Log**.




Type	Date	Time	Message
Status	2019/09/12	15:14:20	TNBTMON (PSQL AuditMaster) is ALIVE on ZEN-SERVER at 2019/09/12 [15:14:20]
Status	2019/09/12	15:14:20	Starting PSQL AuditMaster(R) server processes...
Status	2019/09/12	15:14:20	Registering files...
Status	2019/09/12	15:14:20	Number of Tables Registered: 0
Status	2019/09/12	15:14:20	* Actian AuditMaster(R) v14.0.0 Configuration *
Status	2019/09/12	15:14:20	- Config files path : C:\PROGRAMDATA\ACTIAN\ZEN\AUDIT\DATA\

As in the Audit Records tab, this tab offers icons for working with the content displayed. In the following table, the searching, exporting, and displaying of columns work the same as in the Audit Records tab, and links to those topics are provided. Instructions for filtering and sorting messages are given here.

Command	Description
Filter Log Messages 	Filter the status log messages displayed by type and date. Status and error messages are displayed by default. You can choose to display debug messages as well.
Export 	Exports a current or archived view file to a text file. Exporting from the Status Log tab works in the same way as described under Exporting Audit or Log Records to a Text File .
Search 	Searches for specific text in the Status Log tab. For details, see Searching Audit or Log Records .
Refresh status messages 	Updates the list of logged status and error messages in the Status Log tab.
Select Columns to Display 	Chooses which columns appear in the tab.

To filter and sort status log messages

1. Open the Status Log tab.
2. Click the filter icon .
 - To filter by type of message, select Debug, Error, Status, or a combination.
 - To filter by specific dates, select the check box for **Earliest** or **Latest** or both and set a date range. If neither of these is selected, then the default range is from the earliest to the latest record in the current display.
3. When you are finished setting filter options, click **OK**.
4. You can sort messages by clicking the header of the column to use for sorting. To return the sort order to the default, close and reopen the tab.

Disabling and Enabling the Monitor

During certain procedures, such as bulk loading of records, it may be preferable to stop monitoring a database temporarily because the expected large volume of audit records does not offer the same value as in routine monitoring. In these cases, you can manually disable the AuditMaster monitor, perform procedures, and then reenable it to return to auditing normal activities.

Note: You can use these steps only locally on the same machine as the monitored Zen server.

To disable AuditMaster monitoring on an audit server

1. Log in to AMCC as an AuditMaster user with administrative permissions.
2. Under Audit Servers, right-click the name of the machine to be disabled, next to which the message "(Monitor running)" appears.
3. Select **Disable Monitor**.
4. When you are prompted to restart the Zen engine service, click **Yes**.

The message next to the machine name changes to "(Monitor disabled)." You may now perform database procedures that would have been captured as audit records.

When you are finished, use the following steps to restore auditing:

To enable AuditMaster monitoring on an audit server

1. Log in to AMCC as an AuditMaster user with administrative permissions.
2. Under Audit Servers, right-click the name of the machine to be enabled, next to which the message "(Monitor disabled)" appears.
3. Select **Enable Monitor**.
4. When you are prompted to restart the Zen engine service, click **Yes**.

The message next to the machine name changes to "(Monitor running)." Database activity is now again being monitored according to the audit configurations that have been set.

Maintaining Users

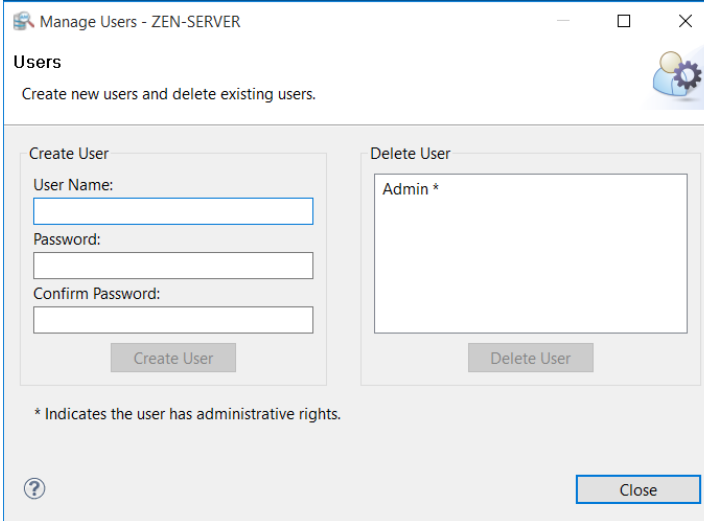
As part of AuditMaster security, users must be authenticated to gain access to the AuditMaster system. As administrator, you define user names and provide a password for each user. You also decide whether each user has administrator privileges.

This topic covers tasks done in the User Maintenance window.

- [To add a user](#)
- [To remove a user](#)

To add a user

1. Select **Admin > User Maintenance** or click the  icon in the tool bar.



The screenshot shows the 'Manage Users - ZEN-SERVER' window. It has a title bar with standard window controls. Below the title bar, the word 'Users' is displayed, followed by the instruction 'Create new users and delete existing users.' and a user icon with a gear. The window is divided into two main sections: 'Create User' on the left and 'Delete User' on the right. The 'Create User' section contains three text input fields labeled 'User Name:', 'Password:', and 'Confirm Password:', each followed by a 'Create User' button. The 'Delete User' section contains a list box with 'Admin *' and a 'Delete User' button. At the bottom, there is a note '* Indicates the user has administrative rights.' and a 'Close' button.

2. In the Manage Users window, enter a user name and password. User names are not case sensitive, can be up to 20 characters long, and can include spaces. Passwords are case-sensitive and can be up to 40 characters long. For double-byte character sets, the user name and password lengths are 10 and 20 characters, respectively.
3. Click **Create User**.
4. You are asked whether to give this user AuditMaster administrator privileges. Click **Yes** or **No**.

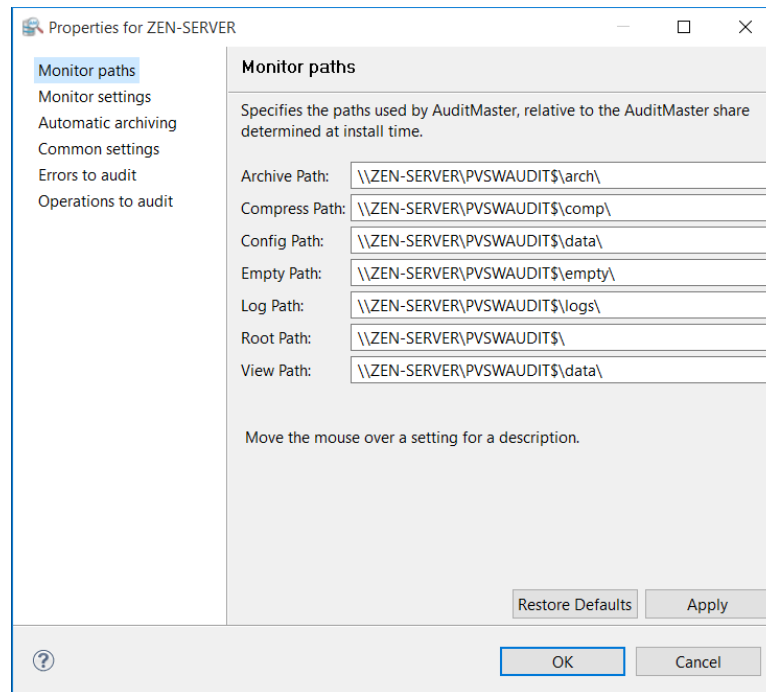
The new user appears in the list on the right.

To remove a user

1. Select **Admin > User Maintenance**.
2. In the Manage Users window, select a user in the Delete User list and click **Delete User**.

Maintaining Server Settings

The Server Settings window displays AuditMaster options. You can open it using the **Admin > Server Settings** command.



The window offers groups of settings. As shown in the following table, some of the settings can be changed, although in most cases this is not needed.

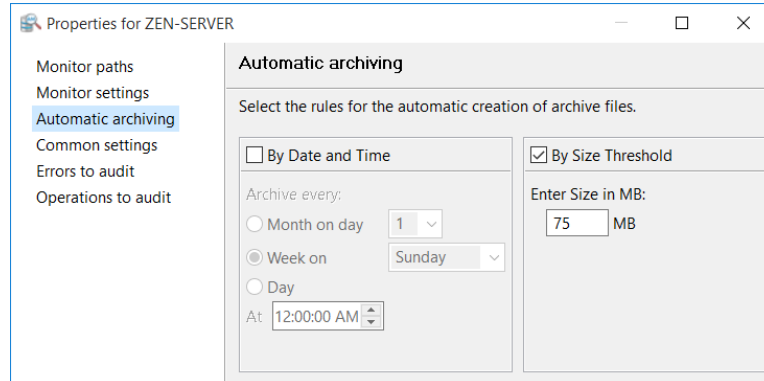
For changes to take effect, you must click the **Apply** or **OK** button. Also, except for automated archiving, the Zen database engine must restart to activate changed settings.

Setting Group	Setting	Purpose
Monitor paths	Various path names	These locations are set at installation time to work with a shared volume that is also created by the AuditMaster installer. In most environments the default paths can be left as is. However, to meet security requirements the share can be manually replaced with an explicit local path name. For instructions, see Replacing the Network Share with a Local Path . Be advised that doing so blocks remote clients and restricts access to only the local system.

Setting Group	Setting	Purpose
Monitor settings	Archives to Keep	Used with Automatic Archiving settings. By default, the value is -1 , which means that the system does not limit the number of archive files. If the value is greater than zero, then the system retains only that number of the most recent files and deletes the older ones. Use of this setting may lead to unintentional loss of archived audit records. Be sure to consider the possible situations when it may be undesirable to delete archive files automatically.
Monitor settings	Mapper Threshold	Controls the frequency of automatic refreshing of the Current View File in AMCC. Default is 1, meaning 1 minute. Setting the value to zero turns off automatic refreshing. Its entry in amstatus.log is "Running Mapper after n minute(s)."
Automatic archiving	Creation of Archive Files	Configures the automatic moving of audit records into archive files. For instructions, see Automatic Archiving .
Common settings	Archive Disk Limit	Used with Automatic Archiving settings. By default, the value is -1 , which means that the system does not monitor the total size of all archive files. If the value is greater than zero bytes, then the system retains only the most recent files for which the total size is less than or equal to this number of bytes and deletes the older files. Be sure to consider the possible situations when it may be undesirable to delete archive files automatically.
Common settings	Max Status Log Size	Maximum length in bytes of the amstatus.log file. Default is 10000000 (10 million) bytes. Minimum value is 1024 bytes.
Common settings	Status Log File	Location of the amstatus.log file. The default path uses the AuditMaster share PVSWAUDIT\$, but you can replace it with another location.
Errors to audit	Btrieve Error Codes	Selects the Microkernel Engine status codes to log as audit events. A certain number are turned on by default. See Errors to Audit .
Operations to audit	Default operations to audit globally	For each file to be monitored, sets the Microkernel Engine events to enter by default in the audit log. These settings can be manually changed on each file. See Operations to Audit Globally .

Automatic Archiving

The Automatic Archiving group offers options for configuring audit record archiving.



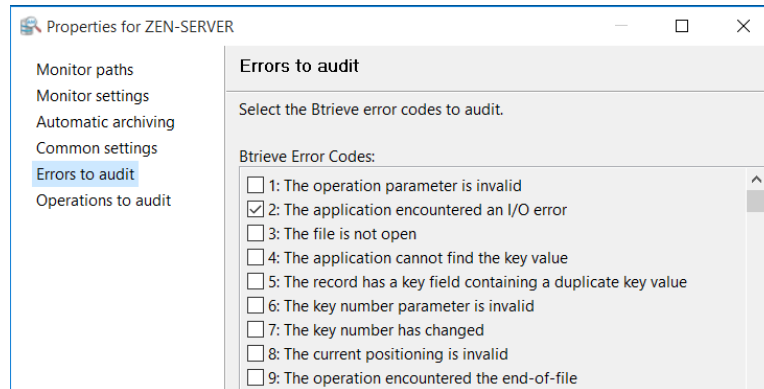
By default, AuditMaster automatically moves audit records to an archive file when audit records in the log file reach 75 MB. Under Admin > Server Settings > Automatic Archiving, you can change this default size, choose to archive by date, or set up a combination of the two. The allowed range for the size threshold is 40–1024 MB.

If you select the check boxes for both By Date and Time and By Size Threshold, then whichever condition occurs first will prompt the system to create an archive file and clear the log file to empty.

If you clear the By Size Threshold setting and choose By Date and Time, the system still uses a 1024 MB size threshold. If the date and time you select has not occurred and the log file size reaches 1024 MB, the system will automatically archive, then when the date and time arrive, it will archive again.

Errors to Audit

The Errors to Audit group lists a set of Microkernel Engine status codes that can be captured as audit events.



For auditing of status codes to work, all of the following must be true:

- The error to be audited is selected in this list.
- The table or file in which the error occurs is assigned to an audit group to be monitored.
- The operation being performed when the error occurs must be an audit operation for the file. For example, to log a status 46 on an update operation, you must have selected Modify Before/After for that table or file.

In the current release, the list of errors has the following codes selected by default:

2, 18, 19, 30, 32, 46, 51, 54, 85, 120, 132, 161, 170, 171

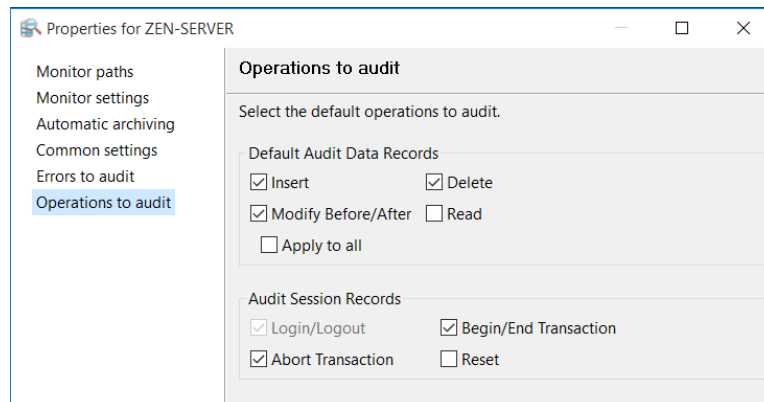
If you do not want audit records captured for a particular error, clear its check box in the list.

For information about the status codes in the list, see *Status Codes and Messages* in the Zen database documentation.

After you make selections from the list, the Zen database engine must restart to activate them.

Operations to Audit Globally

The Operations to Audit window offers the same Insert, Delete, Modify Before/After, and Read events as in the window to create or edit a group under an audit configuration. In addition, you can also audit the session events Begin/End Transaction, Abort Transaction, and Reset. The session event Login/Logout is always audited and cannot be changed.



Unlike settings for individual files, all of these options are global for any file in any audit configuration.

At AuditMaster installation time, the defaults in this window include all operations except Read and Reset. If you select different options, they become the new defaults for any file you add to an audit group. Audit events for previously monitored files are not affected unless you select **Apply to All**.

Finally, if any file is removed from a group and then added again, its operations to audit settings default to the current selections in this window.

For information on individual file settings, see [Operations to Audit by Table or File](#).

After a change is made, the Zen database engine must restart to activate the new setting.

Note: In a Zen database, when the client-side cache engine is turned on, the cache engine reads an entire database page after 8 consecutive reads in anticipation of more reads. The records in the database page read by the cache engine are not audited by the monitor on the server. If auditing requires that every read be captured, verify that client caching is disabled. However, lack of engine caching can reduce database performance. In Zen Control Center, expand **Local Client**, right-click **MicroKernel Router**, and select **Properties**, then click **Performance tuning** to see the setting **Use Cache Engine**. By default, the setting is off.

Replacing the Network Share with a Local Path

AuditMaster installs a hidden network share to enable remote client access for AMCC from other systems. If for security reasons you would like to disable the network share to block remote access, you can replace it with an explicit local path after AuditMaster installation. This replacement can be done only on the server where AuditMaster is installed, not from a remote client. No existing audit records are affected, but auditing must stop momentarily when you restart the monitor to complete the share removal process.

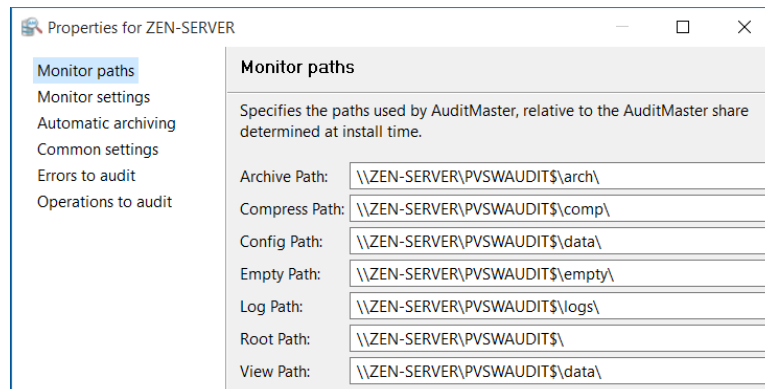
Note: Removing the network share will prevent remote access by all AMCC clients to the AuditMaster system. Be sure that you want to remove it.

To replace the default network share with a local path

1. On the system where AuditMaster server is installed, open AMCC.
2. In the list of audit servers, right-click one and select **Login**.
3. Enter an AuditMaster administrative login name and password, and click **OK**.

Note: The built-in user ID **admin** has the default password **MASTER**. To change this password, see [Changing Your User Password](#). For information on the relation of AuditMaster logins to database and OS logins, read under [Displaying Audit Records under Zen Security](#).

4. Select **Admin > Server Settings**.



5. For each of the monitor paths, select the path name and change

`\\server\\PVSWAUDIT$`

to

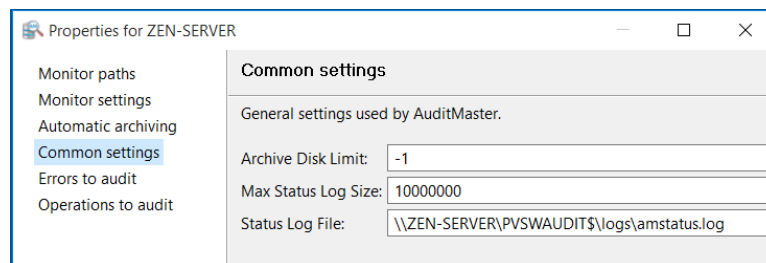
`drive:\\Zen root directory\\Audit`

where *server* is the name of the system on which a Zen server and the AuditMaster monitor are installed and *drive* and *Zen root directory* are, respectively, the local drive letter and absolute path name to the AuditMaster directory selected at installation time.

6. If the default installation location C:\ProgramData\Action\Zen\ has been used, then in this example, the result would be the following:

Archive Path:	C:\ProgramData\Action\Zen\Audit\arch\
Compress Path:	C:\ProgramData\Action\Zen\Audit\comp\
Config Path:	C:\ProgramData\Action\Zen\Audit\data\
Empty Path:	C:\ProgramData\Action\Zen\Audit\empty\
Log Path:	C:\ProgramData\Action\Zen\Audit\logs\
Root Path:	C:\ProgramData\Action\Zen\Audit\
View Path:	C:\ProgramData\Action\Zen\Audit\data\

7. Click the **Apply** button.
8. In the list of options, click **Common Settings** to display values like the following in a default installation:



Properties for ZEN-SERVER	
Monitor paths	Common settings
Monitor settings	General settings used by AuditMaster.
Automatic archiving	Archive Disk Limit: -1
Common settings	Max Status Log Size: 10000000
Errors to audit	Status Log File: \\ZEN-SERVER\PVSWAUDIT\$\logs\amstatus.log
Operations to audit	

9. Select the path name for the status log file and change it to
*drive:**Zen root directory*\Audit\logs\amstatus.log
10. After you have finished changing the values, click **Apply** and then **OK**.
When you are prompted to restart the Zen engine service, click **No**.
11. In AMCC select **Server > Remove** and when prompted to confirm, click **Yes**.
12. Exit AMCC.
In order to remove the network share, AuditMaster and the Zen database engine must be stopped.
13. Open ZenCC and in Zen Explorer, right-click the Services node and select **Stop All Services**.
14. In Windows Explorer, open the folder *drive:**Zen root directory*.
15. Right-click the shared folder Audit and select Properties.

-
16. Select the Sharing tab, then select Advanced Sharing.
 17. Clear the check box **Share this folder**, and click **OK** to delete the share and close Properties.
 18. In Zen Explorer, right-click the Services node and select **Start All Services**.
 19. After the Zen database engine has restarted, add the server back to the data tree using **Server > Add**, as described under [Adding a Server](#).
 20. Verify that AuditMaster is working properly without a network share by opening AMCC to log in.

The new AuditMaster server is now ready to operate without a network share. Other server settings are unchanged. Previously captured audit records captured remain in the system. Only the means of the AMCC client connection has changed.

Basic Troubleshooting

The following topics can help you to resolve common problems that you may encounter:

- [General Tips](#)
- [Troubleshooting Strategies](#)
- [Restarting the Status Log](#)
- [No Records Returned by Query Despite Changes to Application Data](#)
- [Database Engine](#)

General Tips

This topic lists general tips for using AuditMaster.

- When configuring your application data for monitoring, be sure that the files you select reside on the same server as the AM server.
- Be sure that the Zen settings are optimized. Common settings are communication protocols, files, and file handles. Check Zen documentation for information on configuration and optimization.
- AM numbers audit records automatically to an upper limit of 2,147,483,647. After that, numbering wraps and the next audit record starts again at 1. If you notice that the audit record number has suddenly dropped, check to see whether this has occurred.

Troubleshooting Strategies

The following checklist contains items to help you diagnose problems with AM.

- ☐ Does the AM status log contain errors? See [Reviewing Activity in the Status Log](#).
- ☐ Is the Zen database engine running? See [Database Engine](#).

Restarting the Status Log

AuditMaster writes status records in the file **amstatus.log**, located in a default installation under C:\ProgramData\Zen\Audit\logs. This location can be changed by an administrator user under Admin > Server Settings > Monitor Paths. Under certain conditions, such as disk full, AuditMaster may be unable to continue adding status messages to this file, even after the error condition is corrected. To restart the status log, you can export its contents and then delete the log. AuditMaster then starts a new amstatus.log file automatically.

To restart the status log

1. In the AMCC window, select **Admin > View Status Log** to open the Status Log tab.
2. Export the contents of the Status Log tab as described under [Exporting Audit or Log Records to a Text File](#).
3. Exit from AMCC.
4. Stop Zen services.
5. Delete the original **amstatus.log** file from the logs folder in the AM installation.
6. Restart Zen services.

AuditMaster automatically creates a new status log and makes it available to the current view file.

No Records Returned by Query Despite Changes to Application Data

1. Be sure the AuditMaster monitor is enabled.
 - In the Audit Servers list in AMCC, the Zen server name should be marked "(Monitor running)."
 - The Zen database engine must be running.
2. Check that the application files have been set for monitoring in an audit configuration.
3. If the monitor is running and the files have been configured, be sure to update the view file before querying.
4. Check that archiving has not just occurred, meaning that records of interest are no longer in the current view file.
5. Check both AuditMaster and Zen licenses for activation or expiration, using the License Administrator tool in ZenCC.

Database Engine

The Zen database engine must be running for AM to function.

To verify that the database engine is running

Do one of the following:

- In Zen Control Center, expand the Services node to verify that the Zen database engine is running. If not, right-click that node to select **Start All Services**.
- Or use the following steps:
 1. Open the Windows **Services** management console from the Control Panel.
 2. Look for Actian Zen Enterprise Server Engine.
 3. If it is not started, right-click it and select **Start**.

Advanced Operations

Advanced operations are for those who need utilities and methods for accessing audit data from outside of AMCC.

- [Querying Audit Data Directly through SQL](#)
- [AuditMaster and Client-Side Caching](#)

Querying Audit Data Directly through SQL

The AMCC client and its query builder are not the only means of access to audit records. You also can run direct SQL queries against these records. To do so, you must first use the Query Data-Model Generator (QDMG) utility provided with AuditMaster. The utility generates a script to create a virtual database of views linked to audit records in the AuditMaster system.

Both current view and archived audit records can be queried directly using the query data-model method. Direct queries can support applications to create reports or otherwise display audit records, as well as serve development and debugging purposes.

Use cases are provided to demonstrate how to apply the direct query method to the Demodata database included in the Zen installation.

This topic covers the following items:

- [Query Data-Model Generator Utility](#)
- [Creating a Virtual Database](#)
- [The Structure of an Audit Record](#)
- [Running a Query on the Current View File](#)
- [Running a Query on an Archived File](#)
- [Summary of Direct Query Methods](#)

Note: In AuditMaster 12, internal log and settings files are secured and encrypted with a Zen long owner name, so the SQL query method described here is not supported. However, you can still query audit records created in all other versions.

Query Data-Model Generator Utility

The Query Data-Model Generator (QDMG) utility generates a script, consisting of a set of SQL statements, to run against an empty database. The script populates this virtual database with views that link to audit records stored in the AuditMaster log file. Once the views are created, you can then run queries against them to return results from audit records within AuditMaster.

Syntax

```
qdmg -d DDF_path [-m password] -p name -o file [-l logfile] [-a folder]
```

Options

Option	Description
-a	Data directory on remote server where the amserver file resides. Optional if amserver resides on the same system as the client.
-d	Path name of database schema (.ddf files) to import
-m	Master password if database is secure
-p	Name of audit configuration. For example, Zen Demo. For names with spaces, enclose in quotation marks.
-o	Path and file name of output (.sql) file for generated SQL. If no path name is given, the file is written to the current directory.
-l	Log file name for QDMG messages. Default is amlog.
-h	Help

The log file contains records for the current view file in AMCC. You can also access audit records in archive files, but queries on the current view file must be enabled first. Follow these short procedures in the order given:

1. [Creating a Virtual Database](#)
2. [Running a Query on the Current View File](#)
3. [Running a Query on an Archived File](#)

Creating a Virtual Database

This task gives the steps for using the **qdmg** utility to create a virtual database for direct queries of audit data. The example uses the Demodata database installed with Zen.

1. Before setting up a virtual database, import the schema for your audited database into AM. If this already has been done, go to the next step.

In this example, importing has already been done for Demodata as part of the AM installation.

If you need instructions to import the schema from your own database, see [Managing Schemas](#).

2. Creation of the virtual database will require access to the DDFs of the database for which you want to query audit records. To find this path, do all of the following:

-
- Open Zen Control Center and expand the branch for the database being audited, Demodata.
 - Open the Tables branch for Demodata, right-click on a table, and select **Properties**.
 - Note the Dictionary Path where the DDFs are located.
 3. For the virtual database to link to audit records, you must indicate which audit configuration in AM will be used. To check its name, do both of the following:
 - Open AMCC and log in as an AuditMaster administrator.
 - In the Audit Configurations list in the Tables tab, find the name of the audit configuration that was entered when you imported its schema. In this example, the name is “Zen Demo,” which was already imported in the AuditMaster installation.
 4. In Windows Explorer, create a new folder at the same level as the existing Demodata folder.

In this example, we name the folder DemodataV, adding the V for “virtual,” but you can choose your own name. The script to populate the virtual database will be saved here, as well as the database itself.
 5. Now use **qdmg** to generate the script based on the following:
 - Audited database DDF path name (default C:\ProgramData\Action\Zen\Demodata)
 - No password, since Demodata database security is disabled.
 - Audit configuration product name “Zen Demo”
 - Path and file name for output of the generated script.

The command looks like this:

```
qdmg -d C:\ProgramData\Action\Zen\Demodata -p "Zen Demo"  
-o C:\ProgramData\Action\Zen\DemodataV\script
```

6. Open a command prompt window and run the command.

The prompt returns the following message:

```
Query Data-Model Generator Utility for Action AuditMaster  
Copyright (C) Action Corporation 2019
```

```
Query Data-Model was generated into C:\ProgramData\Action\Zen\DemodataV\script.sql
```

Next, create the database in which to run the script.

7. Open Zen Control Center.
8. Under the name of your server, right-click the Databases (Engine) node and select **New Database**.

The Create Database Wizard appears.

9. This example uses the database name DemodataV and the directory you created, C:\ProgramData\Action\Zen\DemodataV.

Note: The virtual database must reside on the same volume as the AuditMaster installation directory. Also, if the original database uses long (V2) metadata, check the box shown for the new virtual database.

10. Click **Finish** to complete database creation.
11. In Zen Control Center, select **File > Open**.
12. In the Open dialog box, navigate to the file script.sql saved earlier in C:\ProgramData\Action\Zen\DemodataV.
13. In the Select Database dialog box, expand the Databases tree, select DemodataV, and click **OK**.

SQL Editor displays the SQL statements in script.sql.

14. Select **SQL > Execute All SQL Statements**.

The statements in script.sql populate DemodataV with views to audit records. In ZenCC you can expand the Views node under the DemodataV database to see what was created.

The virtual database DemodataV now supports queries on audit record columns, as well as on data columns from Demodata.

You may now do any of the following:

- Find out what you can query. See [The Structure of an Audit Record](#).
- Query current audit records. See [Running a Query on the Current View File](#).
- Query archived audit records. See [Running a Query on an Archived File](#).

The Structure of an Audit Record

The columns in an audit record are described in this section. Its structure is representative of the result returned by a query such as `SELECT * FROM vstudent`.

The following facts should be noted in the example:

- Audit columns in the result have the prefix **AMS** and contain audit data.
- After the **AMS** audit data columns, the rest of the row consists of data fields from the audited table and contain values captured from that table at the time of the audit event.

- Many audit columns match query attributes seen in AMCC and Query Builder window tabs.
- All column names are queryable, but some contain internally used codes that are not particularly relevant to human auditing.

Once you have reviewed the audit record structure, see [Running a Query on the Current View File](#) for steps to run a query on the DemodataV example.

The following table compares the columns in an audit record with those displayed in the Audit Records tab in AMCC.

Virtual Database	AMCC	Description
AM\$rec_id	Record No.	Incremental number for audit record
AM\$opdate	Date	Capture date for audit record (e.g., 2023-06-07)
AM\$optime	Time	Capture time for audit record (e.g., 17:04:30)
AM\$dbms_id	—	Internal use
AM\$dbmsverkey	—	Version of Zen system
AM\$opcontextkey	Operation Context	Normal operation (e.g., BTRIEVE) or error
AM\$opcode	—	Internal use
AM\$optext	Operation	Database event. Events can include any item in Operations list of the Did What tab in Query Builder. SQL logins display in this column. Selected Zen status codes also appear here when first selected in the Errors to Audit area of the Server Settings window.
AM\$dep_rec_id	Dependent Record	Record number for an earlier related record: <ul style="list-style-type: none"> • Modify-before record for modify-after record • Begin-transaction record for end/abort transaction record
AM\$prod_id	—	Internal use
AM\$prodverkey	Product Version	As listed in audit configuration for monitored files
AM\$product_name	Product	As listed in audit configuration for monitored files
AM\$comp_id	Database Engine	Either AM Message API (internal use within AM) or Zen
AM\$compverkey	Component Version	Component version, as listed in audit configuration for monitored files
AM\$comp_name	Component	As listed in audit configuration for monitored files

Virtual Database	AMCC	Description
AM\$tab_id	—	Internal use
AM\$tabverkey	—	Same as AM\$compverkey
AM\$table_name	Table Name	File in which event occurred. Same as Tables attribute in Did What tab. The file must be selected for monitoring in an audit configuration. All configured files appear in the Tables list of the Did What tab in Query Builder.
AM\$tabdef_id	—	Internal use
AM\$group_name	Group Name	Group for monitored files in audit configuration. Same as Groups attribute in Did What tab.
AM\$net_id	Machine Name	Machine name or IP address where the event originated. Same as Machine Name attribute in From Where tab.
AM\$net_user_id	User Name	Login ID under which event occurred. Same as user name in Who tab. See Displaying Audit Records under Zen Security .
AM\$process_name	Process Name	Process that was source of audit event. Same as Process attribute in How tab.
AM\$sess_num	—	Internal use
AM\$lic_num	—	Internal use
AM\$mapstate	—	Internal use
AM\$database_name	Database Name	Database in which audit event occurred. Depending on the implementation of the database concept at the level of the event, this value may be “n/a,” not available.
AM\$osverkey	OS Version	Name and version of the operating system where AM server is running
AM\$retcode	—	Internal use
AM\$reserved	—	Internal use
AM\$databufsize	—	Internal use
AM\$len	—	Internal use
<Data Column 1>	—	First data column from table where audit event occurred
<Data Column 2>	—	Second data column from table where audit event occurred
<Data Column n...>	—	Additional data columns...

Running a Query on the Current View File

Before querying for audit records described under [The Structure of an Audit Record](#), be sure to have done the following:

- Run **qdmg** to generate a script to populate a virtual database with views linked to audit records
- Create an empty database
- Execute the script in the database

If you have completed these tasks, you are ready to run direct queries for audit records as shown in the continuing example in this section.

To run a simple query for DemodataV audit records

1. In AM, set the built-in Zen Demo audit configuration to monitor the Student table in Demodata, then in Zen Control Center under Services, restart the Zen database engine to activate the configuration.
2. In Zen Control Center, open the Demodata database, then open the Student table.
In SQL Editor, the default query `SELECT * FROM "Student"` returns all rows.
3. The first row should contain the student ID 190907350. Click the GPA field for this student, change 4.000 to 3.000, and press **Enter**.
4. In Zen Control Center, select **File > New > SQL Document**.
5. When asked to select a database, click **DemodataV**.
6. In the new SQL document, run the following query. You may copy this statement and paste it in SQL Editor.

```
SELECT AM$rec_id, AM$opdate, AM$optext, ID, Cumulative_GPA FROM VStudent
```

The query should return a result like the following:

AM\$rec_id	AM\$opdate	AM\$optext	ID	Cumulative_GPA
637	10/2/2019	Modify Before	190907350	4.000
638	10/2/2019	Modify After	190907350	3.000

Running a Query on an Archived File

This topic refers to the virtual database DemodataV you created under [Creating a Virtual Database](#).

The **qdmg** script sets selected tables in the virtual database to point to audit records in the current view file. The default path for this file is C:\ProgramData\Action\Zen\Audit\data\amlog. As explained in this section, you can reset the path to an archive file if you know its name.

Archived file names are based on creation date, *yyyymmdd.nn*, where *yyyy* is year, *mm* is month, *dd* is day, and *nn* is number of archive file that day, starting with two zeroes. File names end in a capital V. The default folder for archive files is C:\ProgramData\Action\Zen\Audit\Arch.

When an archive file is compressed, it moves to a different folder, the default for which is C:\ProgramData\Action\Zen\Audit\Comp, and the V in the file name changes to Z. When the file is decompressed, it returns to the Arch folder and the Z changes back to V. Queries can run only on uncompressed records.

The method described here uses two SQL scripts:

- The first script sets the virtual database to point to an archive file instead of the current view file.
- The second script resets the virtual database to its original state so that queries again return results from the current view file.

The following steps demonstrate these scripts using the virtual database DemodataV created earlier. The examples are intended to illustrate how you can write your own versions of these scripts.

To reset the virtual database for an archive file query

1. To use these steps, you need an archive file. Open AMCC, right-click the current view file, and select **Archive**.

AuditMaster moves current audit records to an archive file.

2. Expand the Archived Files node, then right-click the node and select **Refresh**.

The newly created archive file appears in the list.

3. Note the name of the file, which in this example is 20160220.00V. If you wish to see that the V is in the file name suffix, look in the archive folder, (e.g., C:\ProgramData\Action\Zen\Audit\Arch).
4. In Zen Control Center, select **File > SQL Document**.
5. When asked to select a database, click DemodataV.
6. In the new SQL document, run all of the following SQL statements. You may copy and paste them in SQL Editor. Use the name of your own archive file instead of 20191015.00V.

```
-- This script resets the virtual database to
-- the uncompressed archive file 20191015.00V.
ALTER TABLE AM$amlog IN DICTIONARY USING '..\Audit\Arch\20191015.00V';
ALTER TABLE Billing IN DICTIONARY USING '..\Audit\Arch\20191015.00V';
ALTER TABLE Class IN DICTIONARY USING '..\Audit\Arch\20191015.00V';
ALTER TABLE Course IN DICTIONARY USING '..\Audit\Arch\20191015.00V';
ALTER TABLE Dept IN DICTIONARY USING '..\Audit\Arch\20191015.00V';
ALTER TABLE Enrolls IN DICTIONARY USING '..\Audit\Arch\20191015.00V';
ALTER TABLE Faculty IN DICTIONARY USING '..\Audit\Arch\20191015.00V';
ALTER TABLE Person IN DICTIONARY USING '..\Audit\Arch\20191015.00V';
ALTER TABLE Room IN DICTIONARY USING '..\Audit\Arch\20191015.00V';
ALTER TABLE Student IN DICTIONARY USING '..\Audit\Arch\20191015.00V';
ALTER TABLE Tuition IN DICTIONARY USING '..\Audit\Arch\20191015.00V';
```

Note: The script alters the table location property for AM\$amlog in the virtual database and also for all of its copies of the data tables found in the audited database. When you write your own version of this script, be sure you do **not** alter the table location property for the following virtual database tables: AM\$Components, AM\$OpList, AM\$Products, AM\$Tables.

7. After the script runs, you may want to select **File > Save SQL Query As** to keep it for reuse, perhaps under a name such as 201015.00V.sql.

The delta query you ran under [Running a Query on the Current View File](#) should now return the same result as when you ran it against the current view, since those audit records have been moved into the archive file to which the virtual database now points.

To reset the virtual database for a current view query

These steps let you run direct queries on the current view file again.

1. In Zen Control Center, select **File > SQL Document**.
2. When asked to select a database, click DemodataV.
3. In the new SQL document, run all of the following SQL statements. You may copy and paste them in SQL Editor.

```
-- This script resets the virtual database to the current view file.
ALTER TABLE AM$amlog IN DICTIONARY USING '..\Audit\DATA\amlog';
ALTER TABLE Billing IN DICTIONARY USING '..\Audit\DATA\amlog';
ALTER TABLE Class IN DICTIONARY USING '..\Audit\DATA\amlog';
ALTER TABLE Course IN DICTIONARY USING '..\Audit\DATA\amlog';
ALTER TABLE Dept IN DICTIONARY USING '..\Audit\DATA\amlog';
ALTER TABLE Enrolls IN DICTIONARY USING '..\Audit\DATA\amlog';
ALTER TABLE Faculty IN DICTIONARY USING '..\Audit\DATA\amlog';
ALTER TABLE Person IN DICTIONARY USING '..\Audit\DATA\amlog';
ALTER TABLE Room IN DICTIONARY USING '..\Audit\DATA\amlog';
```

```
ALTER TABLE Student IN DICTIONARY USING '..\Audit\DATA\amlog';  
ALTER TABLE Tuition IN DICTIONARY USING '..\Audit\DATA\amlog';
```

Note: The script alters the table location property for AM\$amlog in the virtual database and also for all of its copies of the data tables found in the audited database. When you write your own version of this script, be sure you do **not** alter the table location property for the following virtual database tables: AM\$Components, AM\$OpList, AM\$Products, AM\$Tables.

4. After the script runs, you may want to select **File > Save As** to keep it for reuse, perhaps under a name such as currentview.sql.

The delta query you ran under [Running a Query on the Current View File](#) will now return a result for the current view instead of for the archive file.

Summary of Direct Query Methods

This section summarizes the direct query method for audit records:

1. A virtual database can enable direct queries of audit records independently of AMCC.
2. A special script populates the database. Use the Query Data-Model Generator utility **qdmg** to automate the writing of this script.
3. Create a database on the same volume as the AuditMaster installation root (e.g., default C:\ProgramData\Action\Zen\Audit).
4. Run the **qdmg** script in the database.
5. You may now run queries in the virtual database using the views that were created to return audit records from the current view file.
6. To enable queries of audit records in an archive file, use an ALTER script to reset the virtual database to do so.
7. Use a second ALTER script to set the virtual database back to its original state to query the current view file again.
8. Create and save a reset script for the current view file and for each archive file against which you want to run direct queries. In the virtual database, run the script you need before running your direct queries.
9. Remember that archive files must be uncompressed for queries to succeed.

AuditMaster and Client-Side Caching

In a Zen database, when the client-side cache engine is turned on, the cache engine reads an entire database page after 8 consecutive reads in anticipation of more reads. The records in the database page read by the cache engine are not audited by the monitor on the server. If auditing requires that every read be captured, verify that the cache setting is off. However, lack of engine caching can reduce database performance. The behavior occurs only when the threshold of 8 consecutive reads is reached. If 7 reads and then an update occur, no caching occurs and all 7 reads are captured. To see the setting **Use Cache Engine** in Zen Control Center, expand **Local Client**, right-click **MicroKernel Router**, select **Properties**, and click **Performance tuning**. By default, the setting is off.

If you are not auditing Read operations, you do not need to restrict the use of client-side caching.