

Quest[®] Archive Manager for Files 8.9

Auditing Guide



© 2024 Quest Software Inc. ALL RIGHTS RESERVED.

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

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

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

Quest Software Inc. Attn: LEGAL Dept. 4 Polaris Way Aliso Viejo, CA 92656

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

Patents

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

Trademarks

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

Legend

- **CAUTION:** A caution icon indicates potential damage to hardware or loss of data if instructions are not followed.
- **IMPORTANT, NOTE, TIP, MOBILE OR VIDEO:** An information icon indicates supporting information.

Quest[®] Archive Manager for Files Auditing Guide Updated March 2024 Version 8.9

Contents

Introduction	4
Installation	5
Configuration	9
Configure Database	
Configure Log targets	14
Activate auditing	21
Add audit users	22
Configure auditing service	23
Start auditing service	23
Auditing in ArchiveWeb	24
About Us	27
Contacting Quest	27
Technical Support Resources	

Introduction

1

Auditing is a component of Archive Manager for Files. It allows the administrator to log all actions in the Archive Manager Administration Center and ArchiveWeb.

Installation

Requirements

NOTE: If *Express installation* was used to install Archive Manager for Files, the auditing database must be configured with the Configuration tool. If *Advanced installation* was used to install Archive Manager for Files, the database configuration is done automatically.

Supported databases:

- SQL Server 2016 or higher
- Azure SQL Database
- Oracle 19c or higher

The database will be configured after the installation using the Configuration tool (as described later).

Installation

Auditing can be installed on the Archive Manager server or on a separate machine. The instruction presented here assumes that the Auditing feature will be installed on the same server where the Archive Manager server is installed.

- 1. Login to the Archive Manager for Files server with the credentials of the superuser.
- 2. Run the Archive Manager setup. the default path is C:\Quest\Archive Manager Installation Package\Files\Archive Manager for Files Setup.exe
- 3. Allow the system checks to complete.
- 4. From the *Welcome* window select **Modify**.

Archive Manag	er For Files X
Welcome Modify, repa	air, or remove the program.
	the Archive Manager for Files Setup Maintenance program. This program lets the current installation. Click one of the options below.
Modify	
	Select new program features to add or select currently installed features to remove.
⊖ R <u>e</u> pair	Reinstall all program features installed by the previous setup.
O <u>R</u> emove	Remove all installed features.
u istailor ileitu ——	< Back Next > Cancel

5. Click **Next**. The *Select Features* window opens. Select the **Auditing** check box.

Archive Manager For Files	×
Select Features Select the features setup will install.	
Select the features you want to install, and deselect the Server Service Server	e features you want to uninstall. Description Auditing service of the Archive Manager allows to log all actions made in the Archive Manager console and Archive Web. Administrator has an overview of user actions as archiving, retrieving, restoring and even started full-text searches.
0.00 MB of space required on the C drive 91047.35 MB of space available on the C drive InstallShield	ick <u>N</u> ext > Cancel

6. Click Next. The Logon Information window opens. Specify the credentials.

Archive Manager For Files		×
Logon Information Specify a user account and password.		
Specify the user account to be used by this applied DOMAIN\Username.	cation. User accounts r	nust be in the format
Username:		
democorp\domadmin]
Password:]
Co <u>n</u> firm password:		_
•••••]
InstallShield		-
	< <u>B</u> ack <u>N</u> ext	> Cancel

7. Click **Next**. The *Firewall Settings* window opens. Select the check box to allow communications through server firewalls.

Archive Manager For Files		×
Firewall Settings		
Allow programs to communicate through Wi	ndows Firewall	
InstallShield ————————————————————————————————————	< Back	Cancel

8. Click **Next**. The *Ready to modify the program* window opens.

Archive Manager For Files	×
Ready to modify the program The wizard is ready to begin modify process.	
Click Modify to begin modify process	
If you want to review or change any of your wizard.	settings, dick Back. Click Cancel to exit the
InstallShield	< Back Modify Cancel

9. When the Auditing feature is installed, the *Maintenance Complete* window opens.

Archive Manager For Files	
	Maintenance Complete
	InstallShield Wizard has finished performing maintenance operations on Archive Manager for Files.
	< <u>B</u> ack Finish Cancel

10. Click Finish.

Configuration

In this chapter:

- 1. Configure Database
- 2. <u>Configure Log targets</u>
- 3. Activate auditing
- 4. Add audit users
- 5. Configure auditing service
- 6. <u>Start auditing service</u>

Configure Database

i NOTE: If *Express installation* was used to install Archive Manager for Files, the auditing database must be configured with the Configuration tool. If *Advanced installation* was used to install Archive Manager for Files, the database configuration is done automatically.

In this topic:

- Steps to configure the Auditing database
- Steps to install the Auditing database
- Steps to configure the connection setting

Steps to configure the Auditing database

- 1. When the installation completes, the *Configuration* wizard opens. If it does not open automatically, click **Start > Quest > Archive Manager Configuration**.
- 2. From the feature panel on the left, click Auditing and select the Database tab.
- 3. Click Configure. The Database Connection Wizard opens.

Database configuration	×
Database Connection Wizard	?
The Database Connection Wizard will help you to set up your server. It allows you to specify the database provider and describe the database connection parameters.	
Please select the database provider you want to use:	
Microsoft SQL Server	
C Oracle	
The following page will let you specify the database connection parameters.	
< Back Next > Car	ncel

4. Select either Microsoft SQL Server or Oracle and click Next. If you choose Microsost SQL Server, the Database Connection window opens for the Microsoft SQL Server connection information.

Database configuration	×		
Database Connection Wiza	ırd 🤯		
Set up your Microsoft SQL Server connection.			
Please enter parameters which will be used to create a connection to your Microsoft SQL Server.			
Server name:	AMXDB		
Initial catalog:	MAMAUDIT		
Schema name:	dbo		
Authentication:	Windows Authentication 👻		
Username:			
Password:			
	< Back Next > Cancel		

For Microsoft SQL Server

- a. Server name name of the SQL server (eg. AMXDB)
- b. Initial catalog name of the HSM database (e.g. MAMAUDIT which is the default name of the HSM database)
- c. Schema name name of the SQL Schema (e.g. dbo)
- d. Authentication authentication type used for the database. Choose either Windows authentication or SQL Server authentication
- e. Username database login username if SQL Server authentication is the selected as the authentication mode.
- f. Password password of the database user if SQL Server authentication is the selected as the authentication mode.

For Oracle

- a. **Oracle net name** net service name that describes the network address of the database server in your tnsnames.ora file.
- b. Schema name of the Oracle schema from your tnsnames.ora file.
- c. Username database login username.
- d. Password password of the database user.
- 5. Click **Next** and then click **Yes** on the confirmation dialog that opens.
- 6. If the database connection is setup successfully, the configuration completion window opens.
- 7. Click **Finish** to close the *Database Connection* wizard.

Steps to install the Auditing database

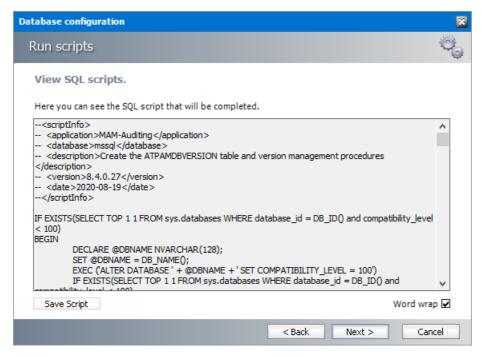
- 1. From the feature panel on the left in the *Configuration* tool, click **Auditing** and then select the **Database** tab.
- 2. Verify that the database connection information is as expected. Then click Run Scripts.

Database configuration		×	
Run scripts		00	
Select scripts to run.			
Please select SQL scripts you want to run.			
🕑 藏 01_audit_version.sql	^	Select All	
🔽 截 02_audit_categories.sql		Unselect All	
🗹 藏 03_audit_computers.sql			
V 🔬 04_audit_methods.sql			
🗹 🥘 05_audit_users.sql			
🗹 截 06_audit_log.sql			
🔽 截 07_audit_indexes.sql	~		
The following page will let you specify the user under which to run database scripts.			
< Back		Next > Cancel	

3. Click Select All and then click Next. The script installer wizard opens.

Database configuration		×	
Run scripts		¢	
Specify the user under which to run database scripts.			
Please specify user under which to run database scripts. The user must be allowed to create or modify tables and procedures in the database.			
Authentication:	Windows Authentication 🔹		
Database user:			
Password:			
☐ I want to see the SQL script before it is run (for advanced users)			
	< Back Next > Can	cel	

- 4. Enter the following information:
 - a. Authentication authentication type used for the database. Choose either Windows authentication or SQL Server authentication
 - a. **Database user** database login username if *SQL Server authentication* is the selected as the authentication mode.
 - b. **Password** password of the database user if *SQL Server authentication* is the selected as the authentication mode.
 - c. I want to see the SQL script before it is run (for advanced users) select this check box to review the SQL scripts.
- 5. Click Next.
- 6. If the I want to see the SQL script before it is run (for advanced users) check box was selected in the previous step the *View SQL Scripts* window opens.



7. Click **Next** or if the **I want to see the SQL script before it is run (for advanced users)** check box was not selected, the *Run SQL Scripts* window opens.

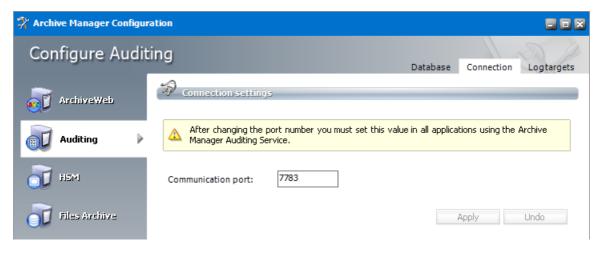
Database configuration	×
Run scripts	0
Run SQL scripts.	
Here you can run the selected SQL scripts to set up the database.	
O1_audit_version.sql	^
02_audit_categories.sql	
O3_audit_computers.sql	
O4_audit_methods.sql	
O5_audit_users.sql	
06_audit_log.sql	
07_audit_indexes.sql	
08_audit_resolvecomputer.sql	~
Click on Next to run scripts.	00:00
< Back Next > C	ancel

- 8. Click **Next**. to run the scripts.
- 9. Click **Finish** to close the script installer. The *Scripts* section of the *Configuration* tool displays the status and version of the scripts(the version of the scripts you install may differ from the version shown in the image below).

🛠 Arch	ive Manager Configu	ıration			
Cor	nfigure Audi	ting		Database	Connection Logtargets
J	ArchiveWeb	Database conn Provider:	ection Microsoft SQL Server		
đ	Auditing		AMXSERVER		
đ	HSM	Initial catalog: Schema name:	MAMAUDIT dbo		
đ	Files Archive	Username:	(Windows Authentication)		Configure
đ	Users	Scripts			
đ	Exchange Archive	Database version: Scripts version:	8.5.0.27 8.5.0.27		
ø	Search	🥝 Your database	is up to date.		
ø	Post Processing				Run scripts

Steps to configure the connection setting

1. From the feature panel on the left in the *Configuration* tool, click **Auditing** and then select the **Connection** tab.



Configure Log targets

In the *Log targets* tab you can configure multiple types of log targets. The default and mandatory log target is the log database. Other targets are optional, depending on administrator's needs. Multiple log targets can be defined and their usage can be conditional. Logging events of

different severity can be logged to different targets or entries containing a specific string can be omitted.

🛠 Archive Manager Configuration 🗧 🖬 🗙			
Configure Audit	Databas	e Connection Logtargets	
ArchiveWeb	Log targets Name Type		
Auditing 🕨 🕨	Database Auditing Database		
可 нэм			
🗊 Files Archive		Add Delete	
可 Users	Log target configuration Threshold level: ALL		
Texchange Archive	Filters: (no filters) Intermediate directory:	Edit Browse	
刻 Search	Flush intermediate files:		
ਗ਼ Post Processing			
		Apply Undo	

Steps to add a new log target

- 1. From the feature panel on the left in the *Configuration* tool, click **Auditing** and then select the Logtargets tab.
- 2. Click Add. The Add log target window opens.

log targe	et and a second s
Name:	
Туре:	Send a message to a user 🔹
	Debug Output Event Log
	File Rolling File Send a message to a user E-Mail

Enter the information as described below:

- a. Name name of the log target.
- b. **Type** type of the log target. Choose from one of the following options:
 - **Debug Output** writes log entries into the debug output; it can be used only for debugging purposes, since it does not keep the entries
 - Event log writes log entries into the system event log; it is recommended to use this target for critical errors and events only
 - File writes log entries into the specified file
 - Rolling File Writes log entries into files and rolls log files based on size or date or both
 - Send a message to a user sends log entries as network messages; it can be used for notification purposes in case of critical errors
 - Email sends log entries as e-mails; it can be used for notification purposes in case of critical errors
- 3. Click **OK** to add the new log target to the *Log targets* list view.

Steps to configure log targets

The target selected in the *Log targets* list can be configured in the *Log target configuration* section. You can configure it in the Log target configuration section. For each log target you can define:

- Threshold level
- Filters
- Layout (not applicable for database)

Additionally, every log target has its specific properties as described further.

Threshold Level

Threshold level specifies the threshold level for the selected log target. All logging events with lower level than the threshold level are ignored. If **Off** is selected, nothing will be logged for the selected target.

Filters

User can define a set of filters for each logging target. Filters form a chain that the logging event has to pass through. Any filter along the way can accept the event and stop processing, deny the event and stop processing, or allow the event on to the next filter. If the event gets to the end of the filter chain without being denied it is implicitly accepted and will be logged.

The available filter types are:

• StringMatchFilter - matches a string (or regular expression) in the rendered message

- **PropertyMatchFilter** matches a string (or regular expression) in the value for a specific event property
- DenyAllFilter this filter drops all logging events

To define a filter for a log target:

- 1. Select the log target in the *Log targets* list view.
- 2. In the *Filters* section click **Edit**.
- 3. In the Edit filters dialog double-click the filter type.
- 4. In the filters options specify filter settings.
- 5. Click Apply.

Edit filters	8
Filters	
Туре	Description
StringMatchFilter	Matches a string in the rendered message
PropertyFilter	Matches a string in an event property
DenyAllFilter	Drops all logging events
Filter chain	
Туре	Filtering rule
PropertyFilter	
	V
	க
Filter options	
String to match	
Regular expression	
Property name	•
Accept on match	
	Apply
)
	OK Cancel

Example:

If you want to allow through only messages that have a specific substring (e.g. 'database') then you need to specify the following filters:

- StringMatchFilter, String to match: 'database', Accept on match: true
- DenyAllFilter

If you do not want to log events having substring 'debug', you need to specify the following filter:

• StringMatchFilter, String to match: 'debug', Accept on match: false

Layout

User can define the layout of a log entry (line) for log targets, except of the Auditing Database. The layout is the sequence of property values separated by arbitrary characters. The available properties are:

- Product product generating the logging event
- Category category of the logging event
- Level level of the logging event
- Message application supplied message associated with the logging event
- Method method name where the logging request was issued
- Data data associated with the logging event
- Computer name of the computer where the logging request was issued
- User name of the user generating the logging request
- Date date of the logging event
- Newline platform dependent line separator character or characters

Specific Log target Properties

Auditing database		
Intermediate directory	For minimizing the logging overhead, this log target operates in asynchronous mode, i.e. the entries are not written into the database directly, but they are held in an internal list and continually written into the database. In case of crash or other unpredictable situations the entries from the memory are lost, so there is an option to persist them to a file. By specifying the intermediate directory the intermediate file creation is activated. For each logging event a file is created, holding the event data. These files are deleted after the log entry was written to the database.	
Flush intermediate files	Determines whether to flush the intermediate files immediately. If this option is set to false, then the underlying stream can defer persisting the entry to a later time, so it is likely that not the whole log entry will be written to the disk when the application exits, thus becoming the entry unusable and lost.	

Event log		
Application name	Specifies the Application name. This appears in the event logs when logging.	
Log name	Specifies the name of the log where log entries will be stored. This is the name of the log as it appears in the Event Viewer tree. The default value is to log into the Application log, this is where most applications write their events. However if you need a separate log for your application (or applications) then you should specify the log name.	
Level mapping	Specifies the mapping between a logging level (severity) and an event log entry type.	

File		
Log file	Specifies the path to the file that logging will be written to.	
File creation	Indicates whether the file should be appended to or overwritten.	
Locking model	Specifies the locking model used to handle locking of the file. When minimal locking is set, the system locks the file only for the minimal amount of time when logging each message. The exclusive locking locks the file from the start of logging to the end.	
Immediate flush	Specifies whether to flush the log file immediately. Avoiding the flush operation at the end of each log writing results in a performance gain of 10 to 20 percent. However, there is safety trade-off involved in skipping flushing. Indeed, when flushing is skipped, then it is likely that the last few log events will not be recorded on disk when the application exits.	

Rolling File	
Log file	Specifies the path to the file that logging will be written to.

Rolling File

Backup file count	Specifies the maximum number of backup files that are kept before the oldest is erased	
Rolling style	 Specifies the rolling style; the possible values are the following: Once - roll files once per program run Size - roll files based only on the size of the file 	
	• Date - roll files based only on the date	
	• Composite - roll files based on both the size and date of the file	
Roll log files by size	Specifies the maximum size in bytes that the output file is allowed to reach before being rolled over to backup files.	
Roll log files every	Specifies the interval when a log file is being rolled over to backup files.	
File creation	Indicates whether the file should be appended to or overwritten.	
Locking model	Specifies the locking model used to handle locking of the file. When minimal locking is set, the system locks the file only for the minimal amount of time when logging each message. The exclusive locking locks the file from the start of logging to the end.	
Immediate flush	Specifies whether to flush the log file immediately. Avoiding the flush operation at the end of each log writing results in a performance gain of 10 to 20 percent. However, there is safety trade-off involved in skipping flushing. Indeed, when flushing is skipped, then it is likely that the last few log events will not be recorded on disk when the application exits.	

Send a message to a user	
Server	Specifies the DNS or NetBIOS name of the remote server on which the Net Send to run.

Send a message to a user	
Recipient	Specifies the message alias to which the message should be sent.

Email	
То	Specifies the e-mail address of the message recipient by semicolon-separated list of e-mail addresses.
From	Specifies the e-mail address of the sender.
Subject	Specifies the subject line of the e-mail message.
Smtp host	Specifies the name of the SMTP relay mail server to use to send the e-mail messages.
Buffer size	Specifies the size of the cyclic buffer used to hold the logging events. When the specified buffer size is reached, oldest events are deleted as new events are added to the buffer. The buffer is used to keep the logging context; when a message is sent, the whole content of the buffer is included.
	If the buffer size is set to a value less than or equal to 1 then no buffering will occur and the messages are sent immediately.

Activate auditing

- 1. Open the Settings tab.
- 2. Check Audit log check box.
- 3. In the **Auditing Server** field enter the name of the computer where Auditing is installed.
- 4. Specify a **Port number** or leave the default.

Archive Manager	ior Files _ 🗆 X
Home AMXSEF	VER
*	Retention categories
Archive	🖏 Default
Scheduler	
Restrictions	
22	Set default Create Change Delete
Settings	Backup time
M	Backup process starts daily at 9:02:09 AM 🚊 and ends at 9:02:09 AM 📑
Statistics	Shortcut creation
	Type of shortcuts to be created Standard Shortcut
	Default action taken when HTML shortcut opened None
	✓ Audit log
	Auditing server AMXSERVER Port number 7783
	Other options
	Track changes in file permissions
	License information Apply Undo
	🚨 General 😔 Notification 🛭 📦 File compression 🛛 🎉 User management 🛛 👸 Storage

Add audit users

As the default, only the super-user has auditing rights, i.e. only the super-user can browse the auditing logs in ArchiveWeb. If you want other users to have access to auditing logs in ArchiveWeb, specific auditing roles must be granted.

- 1. Log on to ArchiveWeb with the super-user credentials.
- 2. Click the logged on user display name in the right upper corner. From the dropdown menu select Manage settings. Then click Roles on the grey sub-bar.

Archive Manager Archive	Veb keyword	search archive	search	retention	report	tasks	Domain Administrator 🗸
Global							Manage settings
							Log Out

- 3. In the left pane select the server for which the roles should apply. Or select **Global** option. ArchiveWeb roles appear in the main pane. List of roles is split into sections – Exchange Archive features are listed under Exchange roles, search features under Search roles etc. The Auditing roles are listed at the end.
- 4. Select the Show auditing logs role. All users with this role are displayed under the list. To add another user, click the Add users and groups icon (🞝) to add it to the list. Then click the Allow toggle.

Archive Manager A	Archive	Web	keyword s	earch		arch	ive sea	rch	retention	report	tasks	Domain Administrator -
ROLES PERMISSIONS	PROFILI	SHARE	D MAILBOXES	TAGS	MANAGEMENT							
Global		GLOB/ ROLES										A
		Ap Au Ex Ex	IG ccess all mailbox oply tags uditor access port auditing lo port results to 2 now auditing log	gs ZIP								
	▼ ▲	de X de	OR USERNA efault emocorp.com\ka emocorp.com\ni	arljordan (k	Karl Jordan) (Niki Portman)							
		L. Ac	dd users or grou	ıps								

Configure auditing service

Finally you need to make sure that the Auditing service is correctly configured. As default it can be found under

<Common Files>\PAM\Services\PAMAuditing\PAMAuditingSv.exe.config

Ensure that the service is using secure channels:

<channels>

```
<channel ref="tcp" name="PamAuditing" port="7783" secure="true" />
```

</channels>

Start auditing service

Open Windows **Services** and start the Auditing service (MAM Auditing) if it is not already running. In case you have made changes to its configuration in the previous step, you must restart it.

Auditing in ArchiveWeb

The Auditing tab is accessible in ArchiveWeb if Auditing is configured properly. Auditing feature allows administrator (or other users defined in web config) to log defined user actions in the email archive, i.e. the administrator has an overview of archived / restored / retrieved emails and performed fulltext searches. Even all actions made in Enterprise Manager console (Exchange / Files) are logged.

To view the logs, from the main pane click Report, then Audit from the grey sub-bar. Then expand the Email Archive node to access the Archive Manager for Exchange logs or Archive Manager for Files node (or "Archive Manager Files Edition" node - both may be present in case older version has been upgraded) to access the Archive Manager for Files logs. Then you can browse through different types of logs – archive actions (Archive node), retrieve actions (Retrieve node) etc.

NOTE: Not all Auditing tab functions may be available for the logged-on user. The functions must be allowed for the user under <LoggedOnUser>/ Manage Settings/ Roles and Permissions sections. For instance, user sees by default only its own search result logs displayed under Email Archive/ Search. Auditors must have Access all mailboxes permission to view search logs of other users (under <LoggedOnUser>/ Manage Settings/ Roles).

Archive Manager Archive	eWeb keyword search	archive se	arch report	tasks Administrator -
STATISTICS AUDIT				
 Archive Manager for Files Archive Configuration 	Result count: 6 Total rows selected: 0 Select all items in folder Drag a column header here to group by that o	olumn		
Search	LOG LEVEL LOG DATE	▼ METHOD	COMPUTER	USER
Settings	Info 07/28/2015 9:27:52 AM	FilePam.Data.DataAcc	AW7	AW\Administrator
Auditing	Info 07/28/2015 9:27:05 AM	FilePam.Data.DataAcc	AW7	AW\Administrator
General	First Prev Page: 1 of 1 Next	Last		
Permissions				
PostProcessing 4	9 Create Filter			
∋ Email Archive	<			>
		10100		
	Product: Archive Manag Category: Settings.Permis Log level: Info Log date: 7/28/2015 9:27 Method: FilePam.Data.D.	ions 05 AM		
< >>	Computer: AW7 User: AW4Administra Message: Permissions up		5	~

NOTE: [OFFLINE] text next to the file server in the left tree-view indicates that the given server has been decommissioned in your environment and is accessible only via

ArchiveWeb. This access must be configured under Manage settings/Profile/File Archive Servers section.

The log entries of the selected action are displayed in the main pane. Data of the log entry selected in the main pane are displayed below the list view (see the screenshot above).

List view functions are the same as in other ArchiveWeb lists:

- Change the column sorting order by selecting the given column header and clicking its down/up arrow on the right (in case the arrow is not visible adjust the width of the column by dragging the line)
- Group table data by any column. To do so, drag the column header to the bar right above the table. Generated groups can be expanded by clicking the arrows next to them. As usual, the sorting order can be changed by clicking the little arrow in the dragged column header.
- Create filters.

Any audit entry can be downloaded or tags can be added or removed from it. All tasks are available through the More actions menu. Click the More actions menu button located on the bottom right just below the list view. Then you can e.g:

- Add tags or Remove tags these options allow you to add or remove tags from selected items
- Export results to ZIP for search results only. This option will export search result items with summary to Excel file and allow to download the created ZIP to user's local machine.
 - **NOTE:** This function is only available if the user has "Export results to ZIP" role allowed for Audit (under <LoggedOnUser>/ Manage Settings/
- Export to XLS this option will export the selected items to XLS file on the user's local machine and provide a download link to the same file.
 - **i** NOTE: When downloading large amount of items it is reasonable to split the data in more XLS files. To do this value for the key "ItemsPerXLS" needs to be changed in ArchiveWeb's web.config file. The default value is "500000" and represents number of rows for single XLS file during the export. In order to set correct value for the key please refer to Excel limits on the page <u>https://support.office.com/en-us/article/excel-specifications-and-limits-1672b34d-7043-467e-8e27-269d656771c3</u>.
- Download log entry: this option will download single log entry in log file format on user local machine.

Archive Manager Archiv	reWeb keywo	ord search	archive s	earch report	tasks Administrat	tor 👻
STATISTICS AUDIT	_					
 Archive Manager for Files Archive Configuration 	Result count: 6 Tot Select all items in fo Drag a column heade		nn			
Search	LOG LEVEL	LOG DATE -	METHOD	COMPUTER	USER	
Settings	🗌 0 Info	07/28/2015 9:27:52 AM	FilePam.Data.DataAcc	AW7	AW\Administrator	
Auditing	🔲 🏮 Info	07/28/2015 9:27:05 AM	AW\Administrator			
General	First Prev Pag	je: 1 of 1 Next La	st			
Permissions						
PostProcessing						
	<					>
	Product: Category: Log level: Log date: Method:	Archive Manager Fil Settings.Permission: Info 7/28/2015 9:27:05 A FilePam.Data.DataA	5	ns	Add tags Remove tags Download log entry	4m)
< >>	AW7 AW\Administrator Permissions update	d			~	

When two or more items be checked, the More actions menu appears automatically under the list view (see the screenshot below).

Archive Manager Archive	eWeb key	yword search	ar	chive	search	report	tasks	Administrator 👻		
STATISTICS AUDIT										
 Archive Manager for Files Archive Configuration 	Select all items in	Total rows selected: 2 n folder Clear selection eader here to group by that col	lumn							
Search	LOG LEVEL	LOG DATE	 METHOD 		COMPL	COMPUTER		USER		
 Settings Auditing 	Info	07/28/2015 9:27:52 AM	FilePam.Da	ita.DataAcc	AW7		AW∖Adn	inistrator		
General	Info	07/28/2015 9:27:05 AM	FilePam.Da	ita.DataAcc	AW7		AW∖Adn	ninistrator		
Permissions	First Prev	Page: 1 of 1 Next	Last							
PostProcessing	9 Create Filter									
	<							>		
			Rem	tags ove tags						
			Expo	ort to XLS						

About Us

5

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

Contacting Quest

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

Technical Support Resources

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

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

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