



**Metalogix Software**

---

# **Auditing**

## **manual**

**v 5.1**

---

*All Rights Reserved, including all rights concerning reproduction, copying or any other use or transmission of this document and its contents or parts of it. No part of this publication may, no matter in what form, be reproduced without written permission by Metalogix Software, passed on to third parties, edited by electronic retrieval systems, copied, distributed or used for public presentations. Metalogix Software reserves the right to change and update the content at any time. All data shown on screenshots is solely for demonstration purposes of the software. Metalogix Software is not responsible for this content.*

*Trademark Archive Manager*

*Microsoft<sup>®</sup>, Microsoft Windows NT<sup>®</sup> and the names of other Microsoft products are registered trademarks of Microsoft Corporation.*

*All Rights Reserved. Other product names are being used for identification purposes of products and can be registered trademarks of the according manufacturers.*

## Table of Contents

<b>Introduction</b> .....	<b>3</b>
<b>Requirements</b> .....	<b>4</b>
<b>Installation</b> .....	<b>4</b>
<b>Configuration</b> .....	<b>5</b>
Database and Log Target Configuration .....	5
Log targets .....	11
<i>Threshold level</i> .....	12
<i>Filters</i> .....	12
<i>Layout</i> .....	13
<i>Specific log target properties</i> .....	14
Enable auditing .....	16
Specifying Audit Users .....	17
Auditing service configuration .....	18
Starting the Auditing service .....	18
Configuring ExchangePamWS .....	18
<b>Auditing in ArchiveWeb</b> .....	<b>21</b>

## Introduction

Auditing server – installed as a feature of Archive Manager Exchange Edition / Files Edition / SharePoint Edition – allows administrator to log all actions made in the Enterprise Manager console.

In case of Exchange Edition it logs also user actions in the email archive, i.e. administrator has an overview of user actions as archiving, retrieving, restoring and even executed fulltext searches (in Outlook and ArchiveWeb).

This manual describes step-by-step all actions you have to take to set up the Auditing correctly. The steps are as follows:

1. If installed with a light setup (not a package), it is necessary to manually create a separate database for Auditing.  
**NOTE:** Archive Manager installation package creates the database automatically.
2. Install the Auditing component.
3. Configure Auditing in the Configuration tool.
4. Enable auditing in the Enterprise Manager. Ensure that the computer name and port, where the auditing service can be found, are correct.
5. Specify Audit users.
6. For version 4.2 and higher – check the Auditing service configuration file <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>
7. Start the Auditing service if not running. If you have made changes to its configuration in the previous step, you will have to restart it.
8. In case of Archive Manager Exchange Edition: Ensure that the ExchangePamWS has anonymous access turned off and Windows integrated authentication turned on.

The above listed points are describe in detail further in this manual.

## Requirements

In case that Auditing is installed with the light Archive Manager Exchange/Files/SharePoint Edition setup (and NOT with the installation package), a separate database for Auditing must be available before installation of the Auditing feature. Supported databases:

- MS SQL 2005 / 2005 Express / 2008
- Oracle

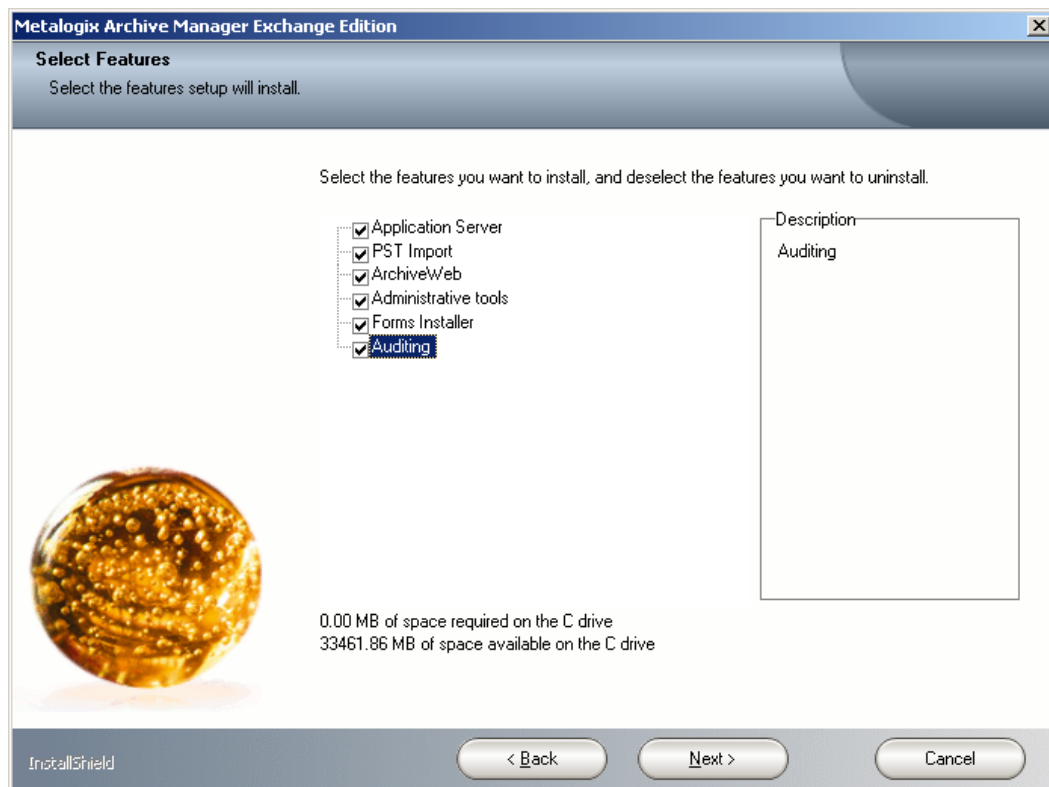
The database will be configured after the installation using the **Configuration** tool (as described later).

At the package installation, Auditing database is created automatically.

## Installation

Auditing feature is installed when you select *Auditing* during the installation of Archive Manager Exchange Edition. In case of Files/SharePoint Edition it is installed automatically.

Auditing can be installed on the Archive Manager server or on a separate machine.



## Configuration

Auditing is configured in these steps:

- I. Database and log targets configuration (in Configuration tool)
- II. Enabling auditing (in Enterprise Manager)
- III. Specifying audit users
- IV. Auditing service configuration (version 4.2 and higher)
- V. Starting the auditing service
- VI. Configuring ExchangePamWS (only for Archive Manager Exchange Ed)

### Database and Log Targets Configuration

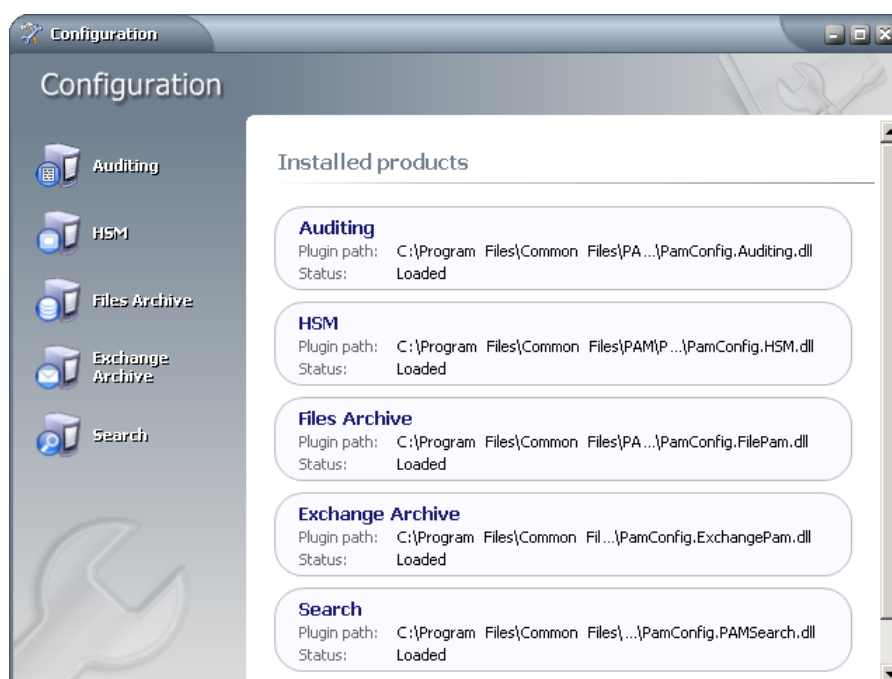
If the light setup was used at the installation, the auditing database has to be configured after installation in the **Configuration** tool.

**NOTE:** If the installation package was used, the database configuration is done automatically. You can use the Configuration tool to specify additional log targets (see the section “Log targets”). If you do not need additional log targets, proceed to the “Enabling auditing” section.

To open the **Configuration** tool, click **C:\Program Files \ Common Files \ PAM \ PAMConfig \ PAMConfig.exe**. The database **Configuration** tool pops-up. This tool administers the database(s) which your Archive Manager software uses to keep meta-data in.

In this manual we use auditDB (with the user `srv_exchange`) as an auditing database.

**NOTE:** The **Configuration** tool can contain several tabs for other databases used by Archive Manager products. However, you need to configure just the Auditing database.



You will notice that each tab of the tool has 2 subsections - the *Configuration* section and the *Execute Scripts* section. Always start with the *Configuration* subsection, since you will first need to set the connection parameters in order to run the sql scripts.

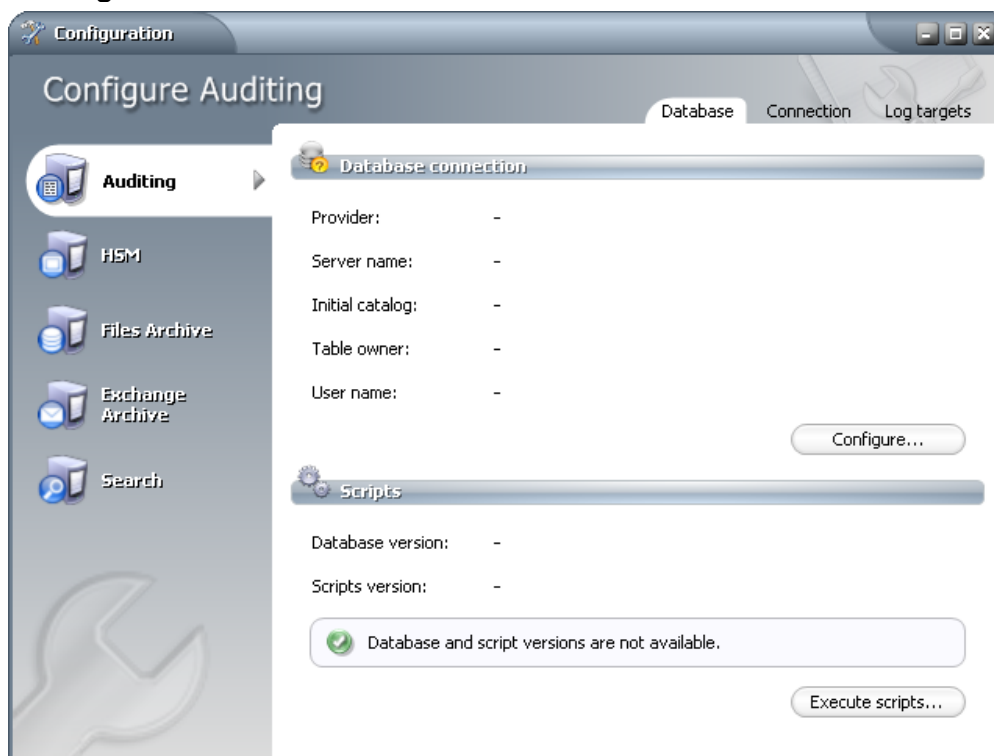
**IMPORTANT NOTE:** Once configured, you **must NOT** change the following values in the **Configuration tool** on any of the tabs:

- **Initial Catalog:** this is the default Database where the system is writing and reading from. This name should never be changed, unless you do not specifically restore all the prior archived data back in Exchange and decide to start all over with a fresh new database for the product. If by mistake another database is used the old archived data is no longer reachable.
- **Table Owner:** this is the default table owner used by the product. This SQL Table owner must be always the same, even if you move the SQL databases from one SQL server to another. If another SQL Table Owner name is created and used for the archiving product all the tables will be re-created as duplicate and the system will write in the new table set. As an end-effect the old archived data will not be reachable anymore. For SQL 2005 / 2008 the Table Owner is the SCHEMA NAME of the database. For SQL 2000 the Table Owner is the SQL login name.
- **Server Name:** this is the name of the SQL server where the databases used by the Metalogix product are hosted. It is only allowed to change this name if the database(s) the Metalogix product uses are moved from one SQL server to another

In case of an ORACLE database, do NOT change **ORACLE NET name** and **Schema**.

To configure the Auditing database:

1. On the database **Configuration** tool switch to the **Auditing** tab and then click **Configure**.



2. If you have an MS SQL server as a database provider, select the respective radio button and click **Next**. If you are using an Oracle database choose the other radio button and click **Next**.



3. In the next window you have to fill in the text fields as follows:

- If you have selected **Microsoft SQL Server**:

**Server name** - the name of the SQL server (or the SQL server instance name if you use SQL 2005 Express).

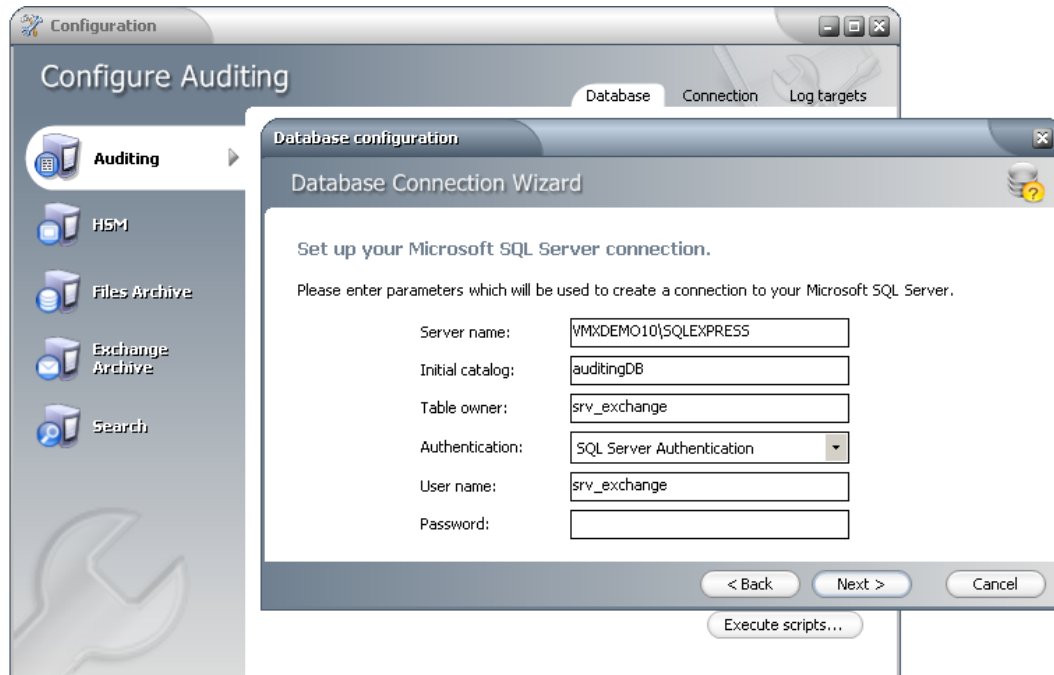
**Initial catalog** - the name of the Auditing database (e.g. *auditDB*).

**Table owner** - the name of the SQL Login that is a Table Owner (or the name of the SQL Schema if you use SQL 2005/2008 Enterprise or SQL 2005 Express), e.g. *srv\_exchange*.

**Authentication** – authentication type used on your SQL server; Windows Authentication is default

**User name** - database login user (the one you are using as a table owner – e.g. *srv\_exchange*)

**Password** - password of the above database login.



**IMPORTANT NOTE:** When updating Archive Manager from one version to another you must NOT change the following values in the Configuration tool on any of the tabs:

- **Server Name**
- **Initial Catalog**
- **Table Owner**

In case of an ORACLE database, do NOT change **ORACLE NET name** and **Schema**.

- If you have selected **ORACLE:**

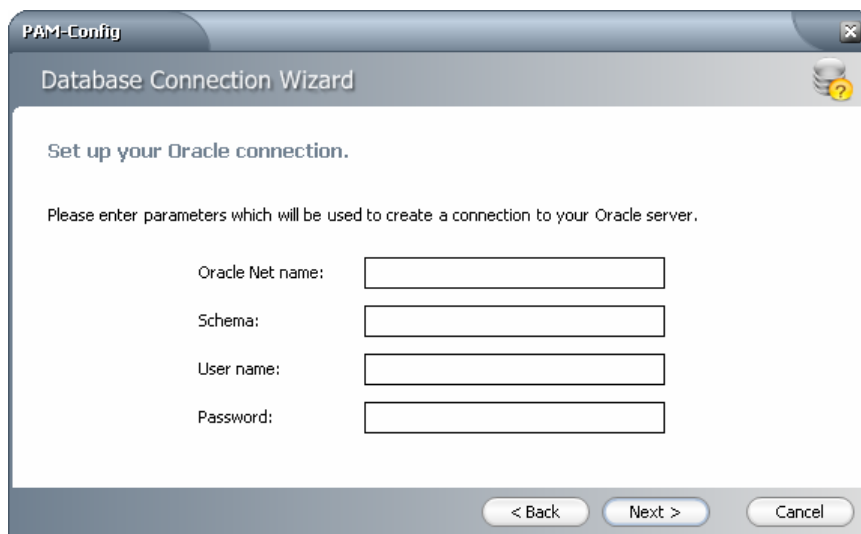
**ORACLE NET Name** - ORACLE NET name, TNS name

**Schema** - the name of the schema where Auditing tables will be created

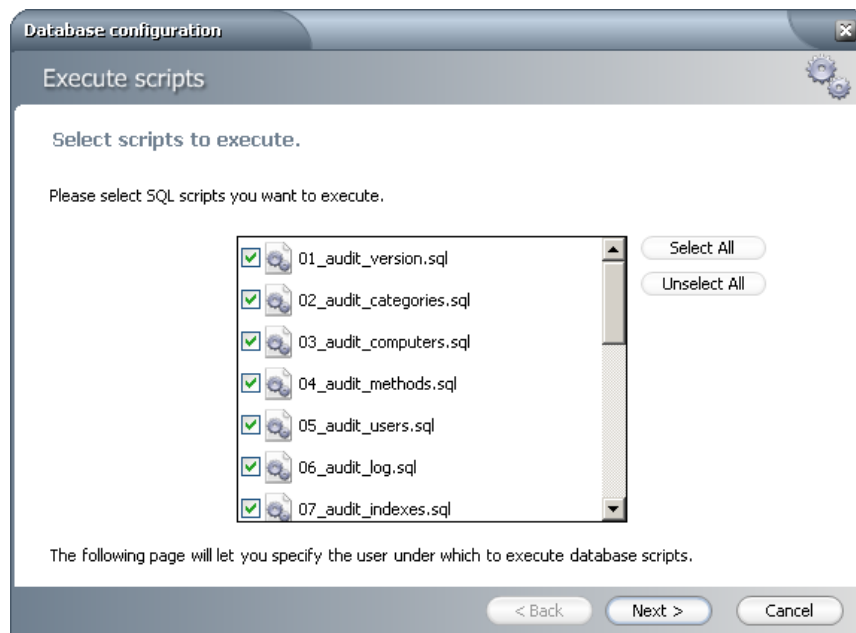
**User Name** - log-on user for the Auditing database (with read and write rights to the tables)

**Password** - log-on user's password

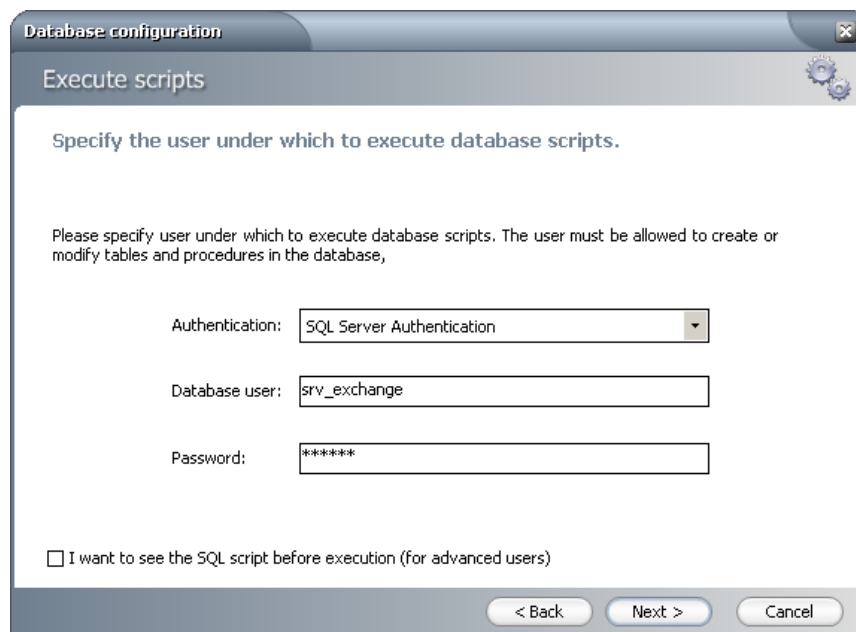
When you have finished, click **Next**. Then **Finish**.



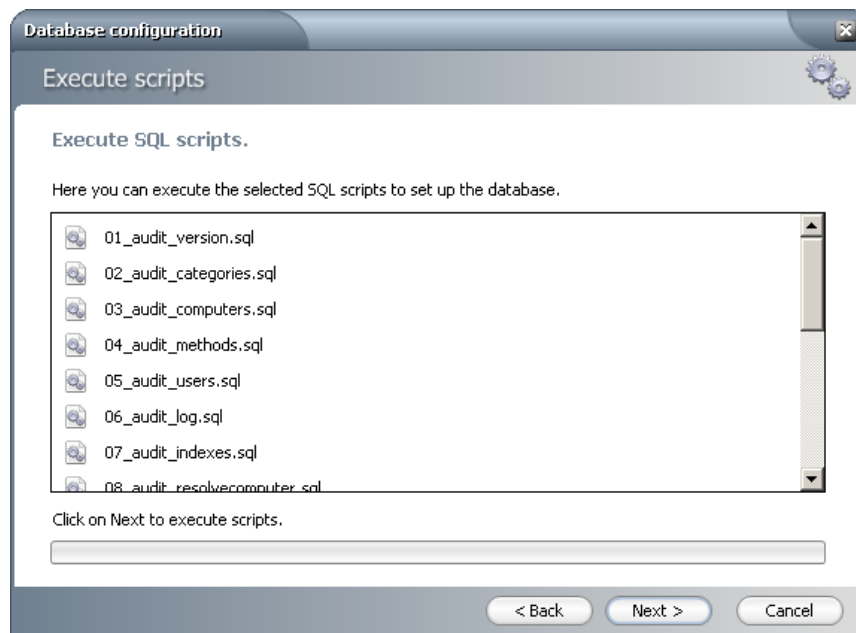
- Back on the **Auditing** tab run the sql scripts by clicking **Execute Scripts**. The list of the scripts will appear. Click **Next**.



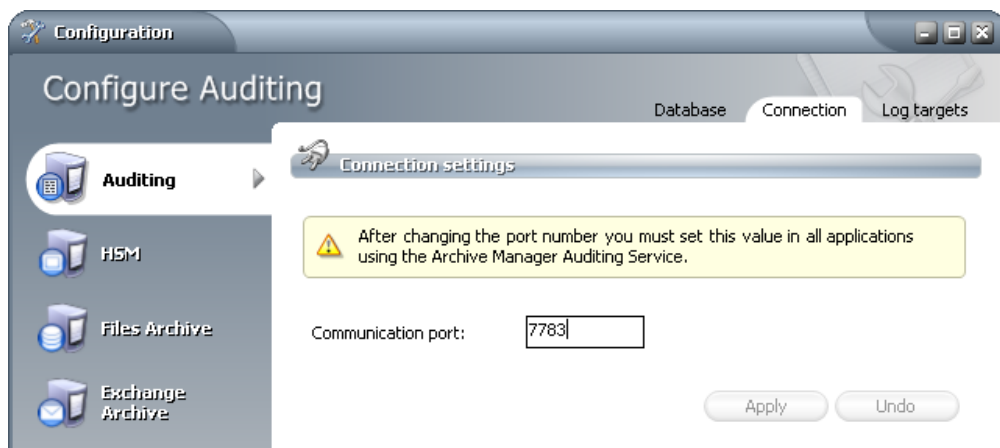
- In case of SQL Authentication, click **Next** once more to accept the database login user and its password.



6. Click **Next** to execute the scripts.

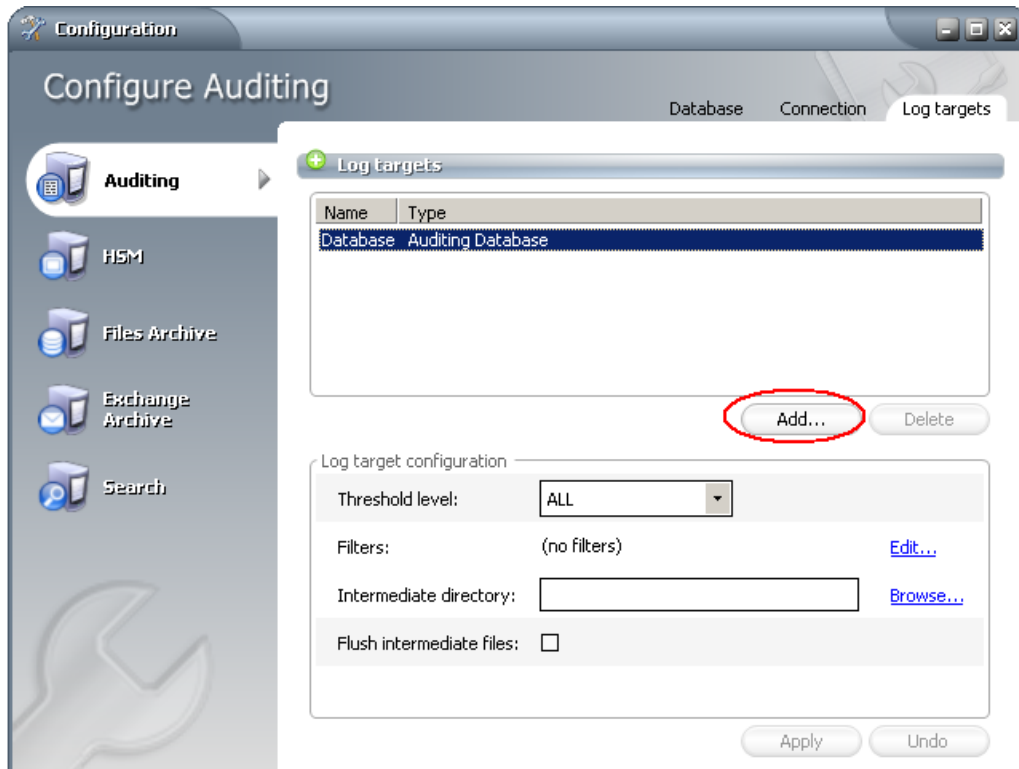


7. On the **Connection** tab it is possible to change the connection port for auditing. However, changing the port is not recommended as this value has to be then rewritten in all applications using the MAM Auditing Service.



8. In the **Log targets** tab you can configure multiple types of log targets. The default and obligatory logging target is the log database. Other targets are optional, depending on administrator's needs.

Multiple log targets can be defined; their usage can be conditioned. Logging events of different severity can be logged to different targets or entries containing a specific string can be omitted (see further).



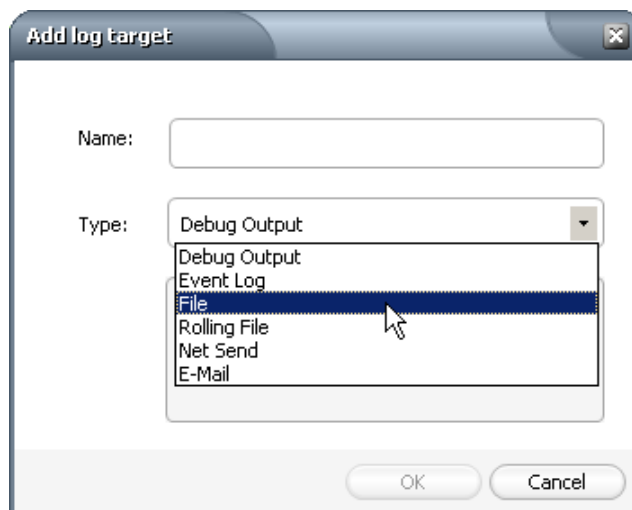
The target selected in the *Log targets* list can be configured in the lower part of the window. Click **Add** button to select a new log target. (Next section deals with log target configuration in detail.)

## Log targets

As mentioned above, log database is default and mandatory log target. Any additional log targets are configured in the Configuration tool (*C:\Program Files \ Common Files \ PAM \ PAMConfig \ PAMConfig.exe*). Click **Auditing / Log targets**. Click **Add** (picture above) to define additional log targets:

- **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

- **Net Send** - 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



In the pop-up window enter the name and select the type of the log target. After clicking **OK**, the log target is added in the *Log targets* list view. 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.

**NOTE:** If „Off“ is selected, nothing will be logged for the selected target.

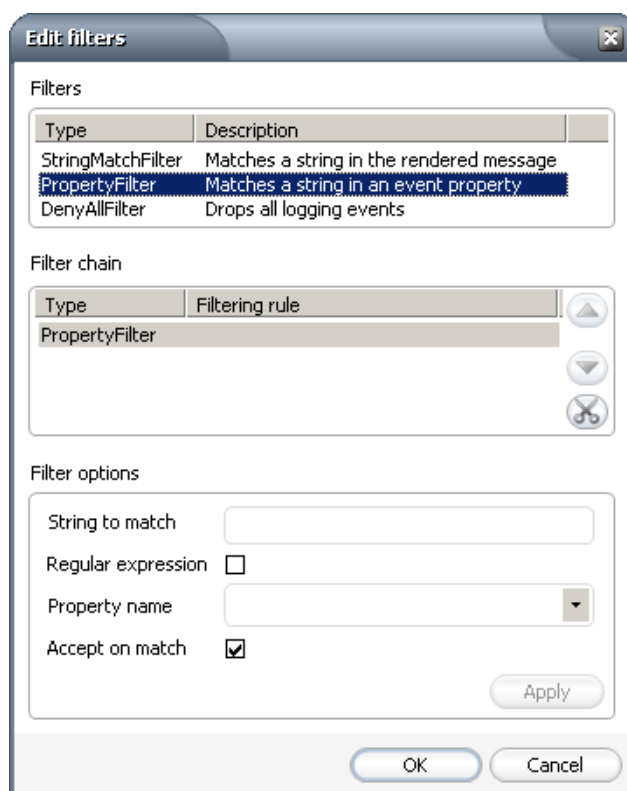
### Filters

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, select the log target in the **Configuration** tool list view. In the log target configuration displayed below, in the *Filters* section click **Edit**. The **Edit filters** dialog pops-up (see the picture below). Double-click the desired filter type. In the filters options specify filter settings. Finally click **Apply**.

**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:

1. StringMatchFilter, String to match: 'database', Accept on match: true
2. DenyAllFilter

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

1. 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	
<b>Intermediate directory</b>	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.
<b>Flush intermediate files</b>	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	
<b>Application name</b>	Specifies the Application name. This appears in the event logs when logging.
<b>Log name</b>	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.
<b>Level mapping</b>	Specifies the mapping between a logging level (severity) and an event log entry type.

File	
<b>Log file</b>	Specifies the path to the file that logging will be written to.
<b>File creation</b>	Indicates whether the file should be appended to or overwritten.
<b>Locking model</b>	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.
<b>Immediate flush</b>	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	
<b>Log file</b>	Specifies the path to the file that logging will be written to.
<b>Backup file count</b>	Specifies the maximum number of backup files that are kept before the oldest is erased
<b>Rolling style</b>	Specifies the rolling style; the possible values are the following: <ul style="list-style-type: none"> <li>• <i>Once</i> - roll files once per program execution</li> <li>• <i>Size</i> - roll files based only on the size of the file</li> </ul>

	<ul style="list-style-type: none"> <li>• <i>Date</i> - roll files based only on the date</li> <li>• <i>Composite</i> - roll files based on both the size and date of the file</li> </ul>
<b>Roll log files by size</b>	Specifies the maximum size in bytes that the output file is allowed to reach before being rolled over to backup files.
<b>Roll log files every</b>	Specifies the interval when a log file is being rolled over to backup files.
<b>File creation</b>	Indicates whether the file should be appended to or overwritten.
<b>Locking model</b>	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.
<b>Immediate flush</b>	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.

Net Send	
<b>Server</b>	Specifies the DNS or NetBIOS name of the remote server on which the Net Send to execute.
<b>Recipient</b>	Specifies the message alias to which the message should be sent.

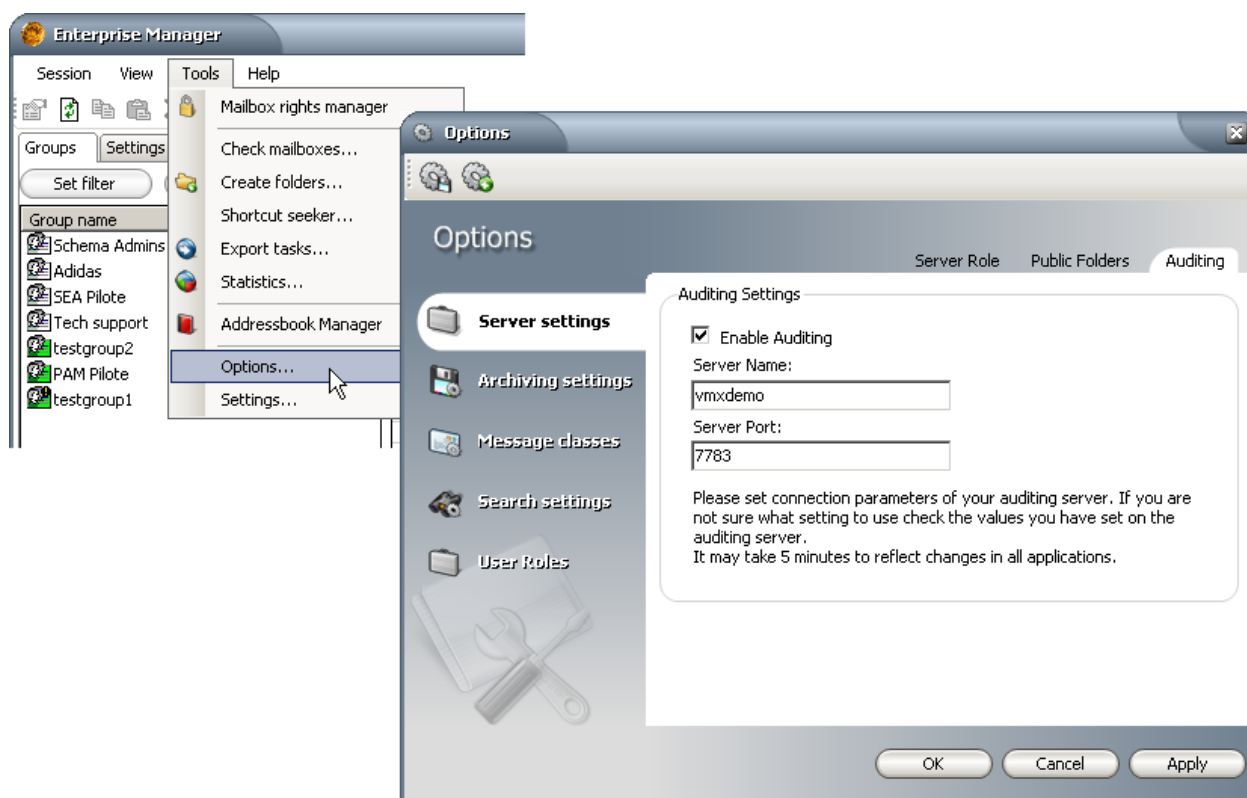
Email	
<b>To</b>	Specifies the e-mail address of the message recipient by semicolon-separated list of e-mail addresses.
<b>From</b>	Specifies the e-mail address of the sender.
<b>Subject</b>	Specifies the subject line of the e-mail message.
<b>Smtip host</b>	Specifies the name of the SMTP relay mail server to use to send the e-mail messages.
<b>Buffer size</b>	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.

## Enable auditing

As a next step, Auditing has to be enabled in the Enterprise Manager.

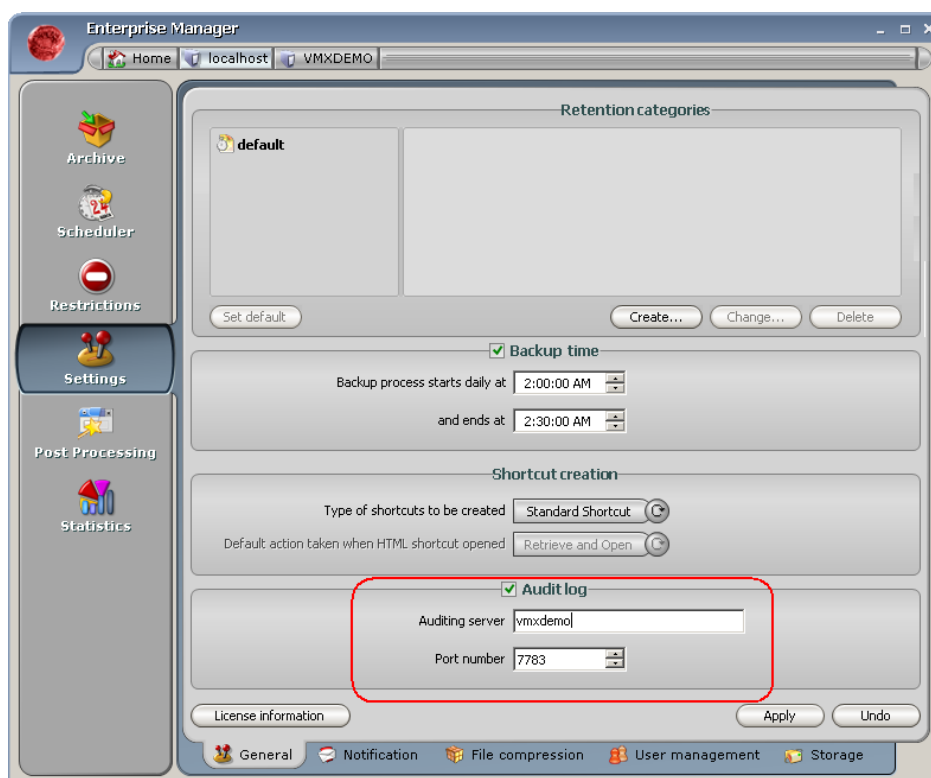
In the case of Archive Manager Exchange Edition Enterprise Manager:

- open **Tools / Options / Server settings / Auditing**. Check **Enable Auditing** check box. In the **Server Name** enter the name of the machine where the Auditing feature is installed and specify the **Server Port**. Click **Apply**.



In the case of Archive Manager Files/SharePoint Enterprise Manager:

- On the **Settings** tab check **Audit** log and enter the name of the machine where Auditing is installed and specify the port; it is 7783 by default

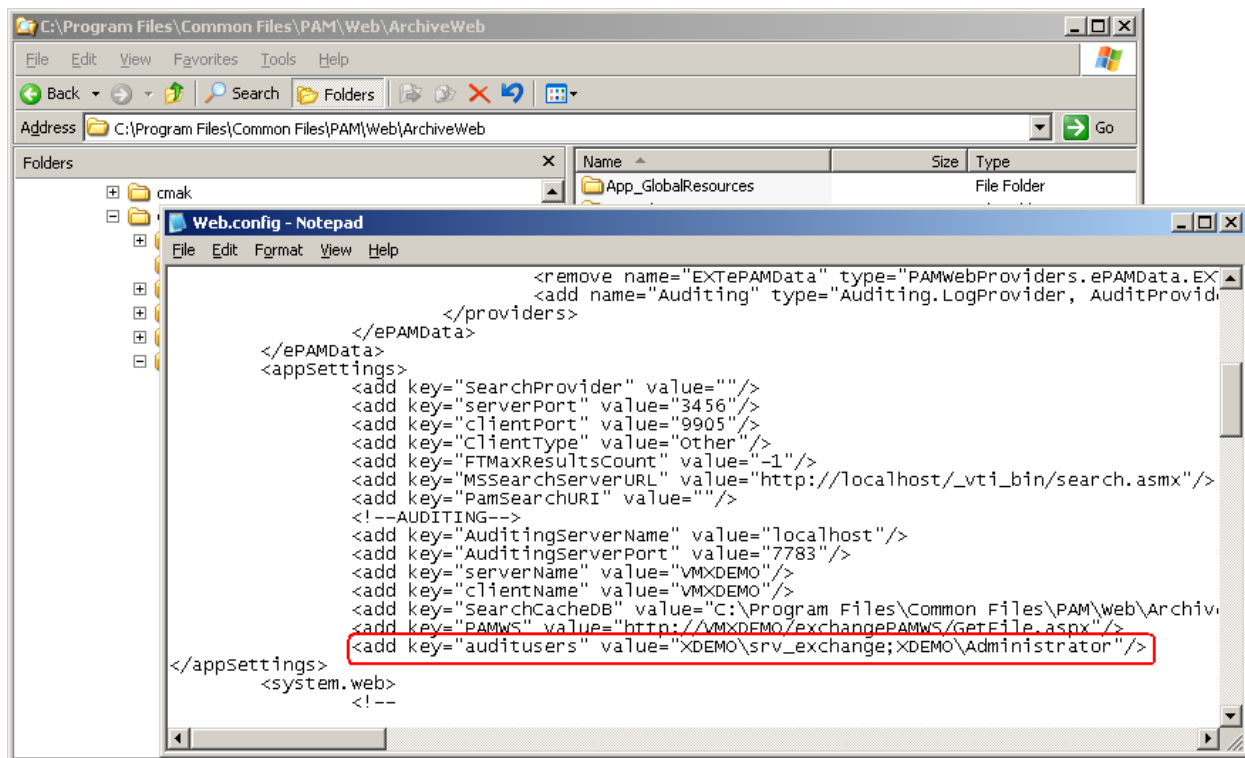


## Specifying Audit Users

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, it has to be configured in the Web config file:

1. Open **C:\Program Files\Common Files\PAM\Web\ArchiveWeb\Web.config**
2. Edit the Web.config. Add users for which you want to allow auditing as *auditusers* in form Domain\User. Use semicolon (;) as a separator.



3. Make sure also that the computer name and port where the auditing service can be found are correct, i.e. that the *AuditingServerName* and *AuditingServerPort* values are correct.

## Auditing service configuration

In version 4.2 you need to configure Auditing service. 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>
```

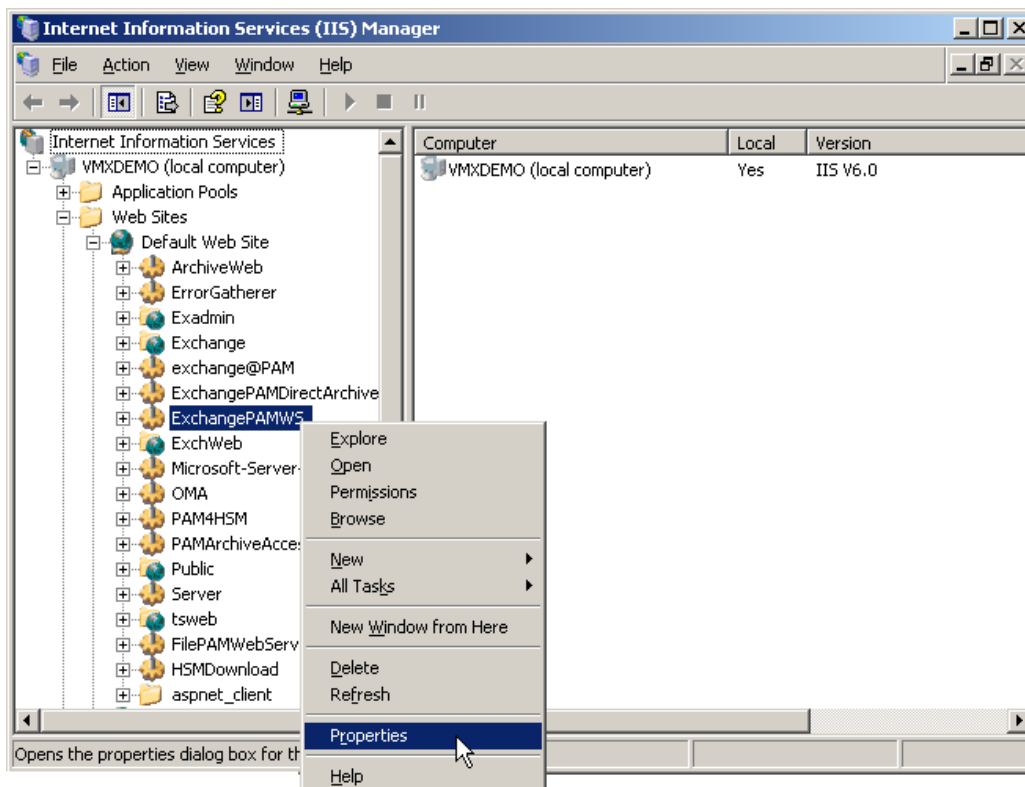
## Starting the Auditing service

Open **Start \ All programs \ Administrative tools \ Services** and start the Auditing service (*MAM Auditing*) if it is not running. In case you have made changes to its configuration in the previous step, you will have to restart it.

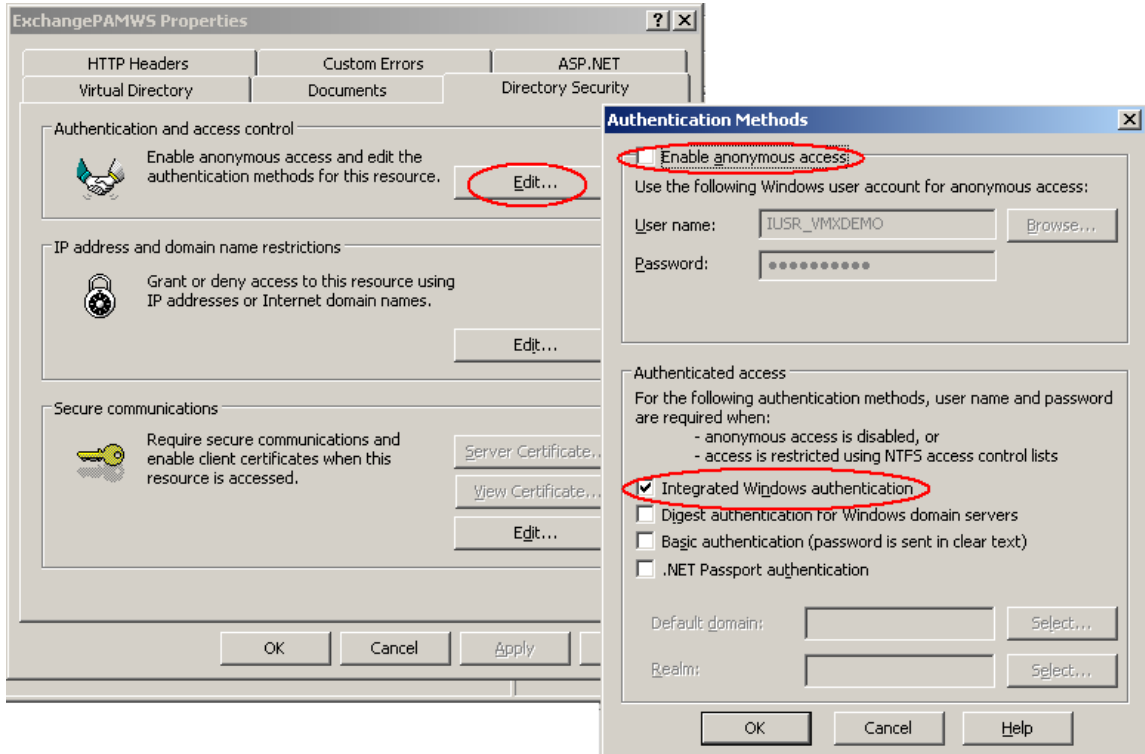
## Configuring ExchangePamWS

In the case of Archive Manager Exchange Edition: Ensure that the ExchangePamWS has anonymous access turned off and Windows integrated authentication turned on on the Archive Manager Server. To do so:

1. Open **Start / All programs / Administrative tools / IIS Manager**
2. In the IIS Manager expand the tree down to **<ComputerName> \ Web Sites \ Default Web Site**. Right-click the **ExchangePamWS** and from the context menu choose **Properties**.



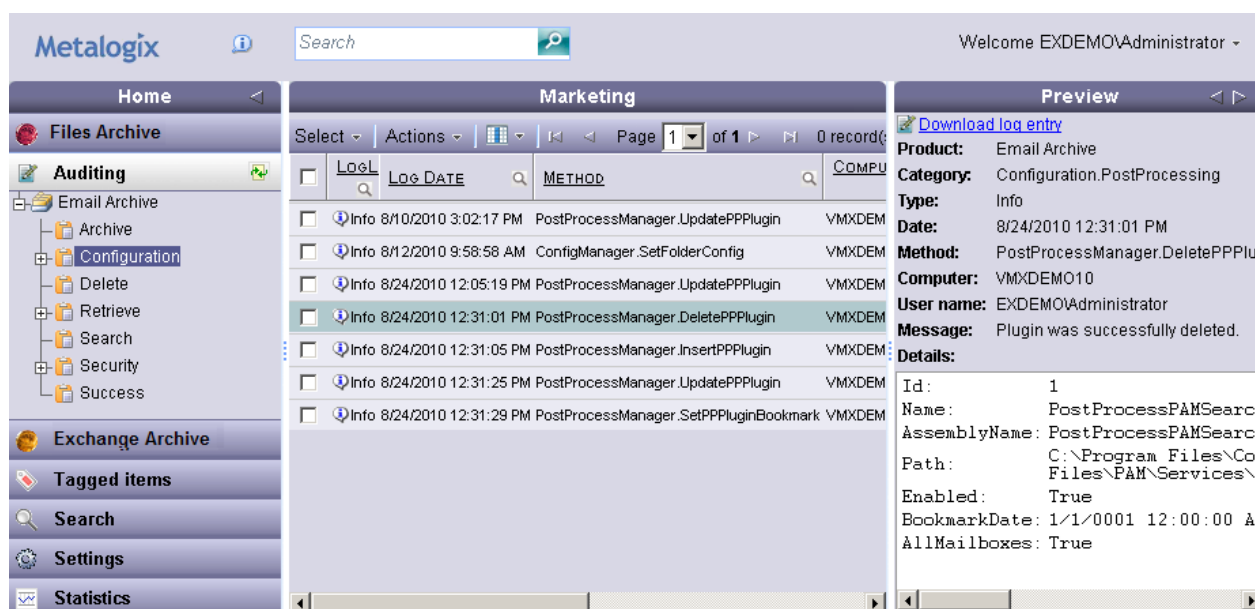
3. In the **Directory Security** tab, **Authentication and access control** click **Edit**. In the pop-up window make sure that the *Integrated Windows authentication* is checked and *Enable anonymous access* is NOT checked.



## 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 executed fulltext searches. Even all actions made in Enterprise Manager console (Exchange / Files / SharePoint Edition) are logged.

To view the logs, click on the **Auditing** tab. Then unfold the **Email Archive** node to access the Archive Manager Exchange Edition logs or **Files Archive** node to access the Archive Manager Files Edition logs. Then you can browse through different types of logs – archive actions (Archive node), restore actions (Restore node) etc.



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 in the **Preview**, e.g. log category, date, computer, user etc.

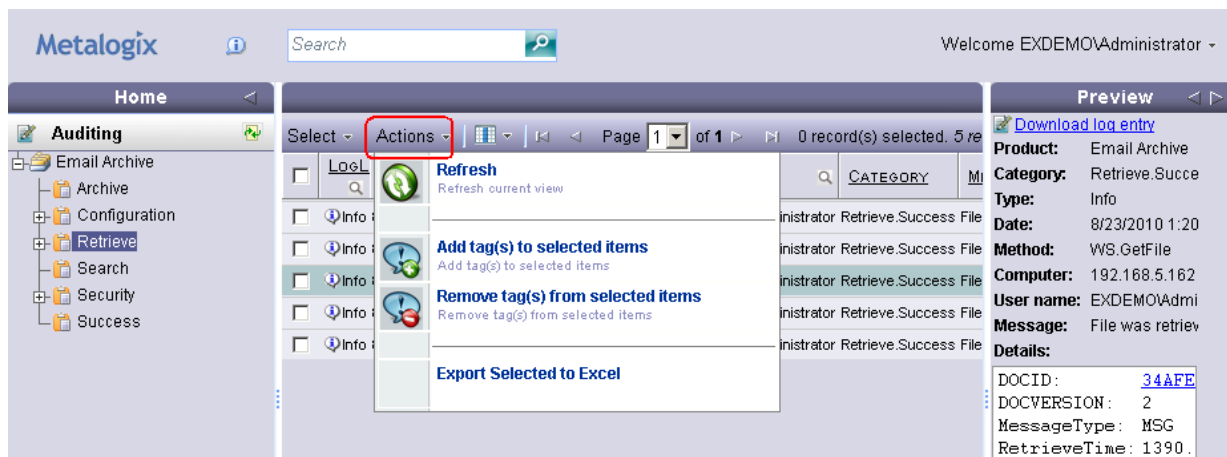
You can download the selected log entry when you click the *Download the log entry* link in the **Preview**.

Filters in the column headers allow you to filter the main pane list view and display only desired items. To apply the filter, click on the search icon (🔍) in the desired column header. In the pop-up dialog set the filter criteria. It is also possible to apply several filters at once.

**NOTE:** Filters are accessible only if they are allowed under the **Your Profile**. To allow filters in the column headers, click the logged-on user name in the right-upper corner. Select **Your profile** from the down-drop menu. Then on the **Style** tab check **Show filters in header** check box. Click **Apply changes**.

The administrator can add tags to log entries, adjust the list view etc. All tasks are available through the **Actions** menu. Hold the cursor over the **Actions** menu button located in the right upper corner to unfold the menu. Then you can e.g:

- **add tags to selected items** (for more information on tags see the “ArchvieWeb manual“)
- **export selected items to Excel**



[www.metalogix.com](http://www.metalogix.com)

Mail Support: [www.metalogix.com/Support](mailto:sales@metalogix.net)

*Metalogix makes every effort to perform comprehensive testing but cannot guarantee, due to environmental differences, that all functions will work in every environment. It is always recommended that testing be conducted within your own environment to confirm functionality and compatibility.*