Quest

Metalogix® Archive Manager for Files 8.3

Hierarchical Storage Manager Guide

© 2020 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 https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

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

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

Metalogix® Archive Manager for Files
Updated November 2020
Version 8.3

Contents

Introduction **4**
Process of archiving using HSM store 4
Installation of HSM **7**
Configuring HSM 8
Creating a MediaStore 18
Jukebox, Hard disk, Network Media Store 18
Simple Path MediaStore 32
Specifying a Schema 39
Optional Configuration **46**
Advanced tab 46
Diagnostics tab 48
Encryption tab 52
Packer tab 55
Tasks tab 57
Addendum **65**
Setting up an MS SQL Server database 65
Remote HSM Server 76
HSM configured for Windows Server firewall 79
About Us **84**
Contacting Quest 84
Technical Support Resources 84

1

Introduction

HSM (Hierarchical Storage Management system), as a data storage systemis a complement of several Metalogix archiving products.

HSM, as a complement of Archive Manager products, can be installed by:

- HSM separate setup
- Installation package of the given Metalogix product (Archive Manager for Exchange Installation package, Archive Manager for Files Installation package etc.)

When installed by the Installation package as a part of the Archive Manager product installation, necessary configuration is performed by the Installation package itself (see the "Archive Manager Quick Start Guide" etc.).

This manual leads you through the HSM installation and configuration when the separate HSM setup is used, i.e. when the Archive Manager product and its components are installed manually.

HSM allows storing of data (even all company data) on one or more file-servers. It is possible to use a shared store as well. HSM includes the Single Instance Store service (SIS), which ensures that identical content is stored only once. The SIS service enables versioning, allowing the HSM system to keep track of any changes made to files or emails. With versioning enabled, the administrator may retrieve older versions. Even if the original file or email was deleted, it can be restored back.

Process of archiving using HSM store

When archived with Archive Manager, the desired file or email with its attachments is transferred to the HSM system. It is the HSM System that takes care of storing and retrieving files/emails. The HSM system works with a database because the information contained in the shortcut is stored either in an ORACLE or MS SQL database. The HSM system passes down the file/email to a store specified by the administrator and this file/email is compressed “on the fly”. Only shortcut of a few kilobytes remains at the file/email’s original location. This shortcut includes information about the new location of the archived file/email. The only difference a user notices is that the shortcut is displayed with a slightly modified icon.

Users may work with archived files/emails as usual which means: when an archived file/email is reopened, Archive Manager passes the information from the shortcut onto the HSM system. The HSM system restores the file/email from the store. For users it seems as if they are working in a normal environment.

The HSM system includes the Single Instance Store service (SIS), which enables versioning in cooperation with Archive Manager products. Due to versioning the HSM system keeps track of any changes made to a document, e.g.:

- **who** modified the document;
- **when** this modification occurred;
- **what** was modified within the document.

With versioning enabled, the administrator may retrieve older versions. Even files whose shortcuts were deleted can be retrieved as well.

The HSM Server (Hierarchical Storage Management Server)

The HSM Server (i.e. the computer where the HSM system is installed), as a complement of Archive Manager products, takes care of saving and securing archived documents. Archived data reside in store. HSM works with different store types depending on administrator's choice.

Supported operating systems:

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2019

Requirements

- **.Net Framework 2.0**
- **.Net Framework 3.5** – if not available, setup can be installed but the following store types will not be functional:

Amazon S3, Windows Azure, Caringo CAStore, EMC Atmos, FileNet IS, Hitachi HCAP, Hitachi HCP, Nirvanix, Rackspace, Simple Foldering Store, XAM

- **.Net Framework 4.5** – if not available, Google Drive store will not be functional.

NOTE: If .NET Framework 4.5 is installed after HSM, it is necessary to run the HSM setup in "Repair" mode to enable the Google Drive store.

- **IIS** (32-bit support) – if not available, setup will continue but the HSM web client will not be installed.
- **Microsoft WSE 3.0** – if not available, the iTernity store cannot be created.
- **Database -** ORACLE Database (version 12c or higher) or MS SQL Server (version 2012 or higher).

General database requirements:

- If you are using an MS SQL Database, then installation of MDAC (Microsoft Data Access Components) is necessary, as it contains the required OLEDB Data Provider for MS SQL Server.

The MS SQL Data Provider for .Net is also needed for accessing MS SQL (part of the .NET Framework installation). We recommend installing the latest version of MDAC (Currently we recommend installing MDAC 2.8.)

- If you are using an ORACLE Database, and it has not been installed on the HSM server, then an ORACLE Database Client must be installed on your HSM server and a Net8 connection from the HSM server to the ORACLE Database server must be established. The ORACLE OLEDB Data Provider (part of the MDAC installation) and the Oracle Data Provider for .Net (part of the .NET Framework installation) are required for connecting the ORACLE Database.

Databases with the database user(s) (who, in addition, should be the owner of the database) have to be available before HSM installation.

Creation of database with a database user in MS SQL 2012 is described in “Addendum – Creating an MS SQL database with a database user”.

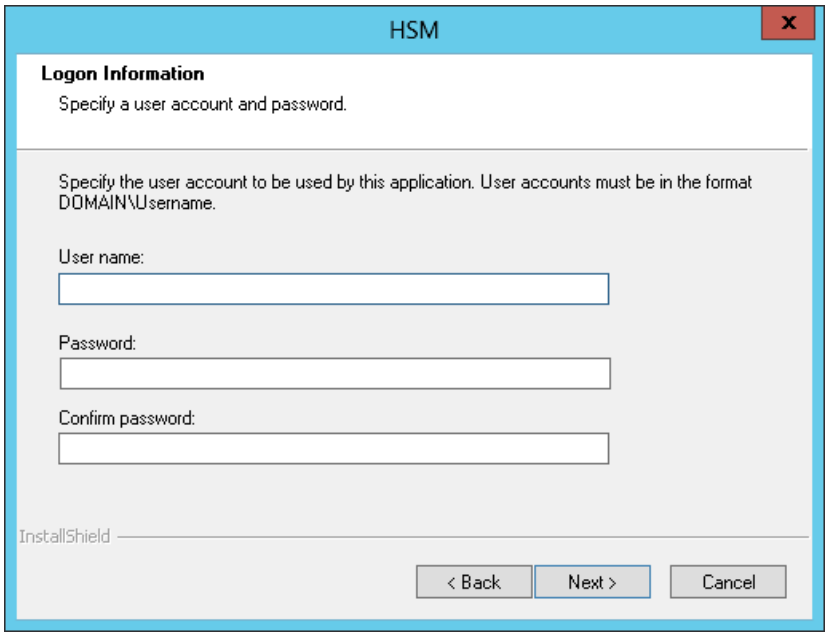
NOTE: If you prefer working with an ORACLE Database, make sure to have similar data (database, database user, password, owner of the schema) available during the installation of Archive Manager for Exchange.

2

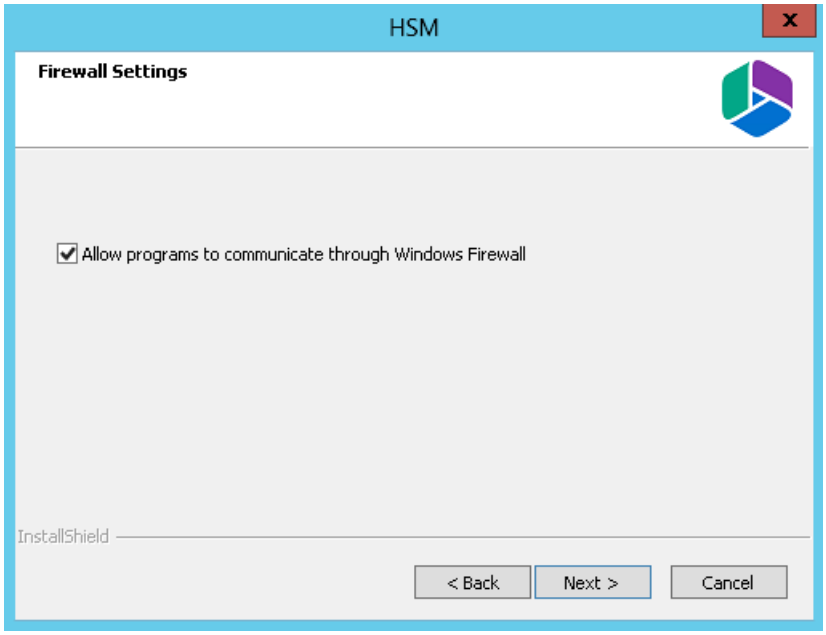
Installation of HSM

To install HSM on your HSM server, follow these steps:

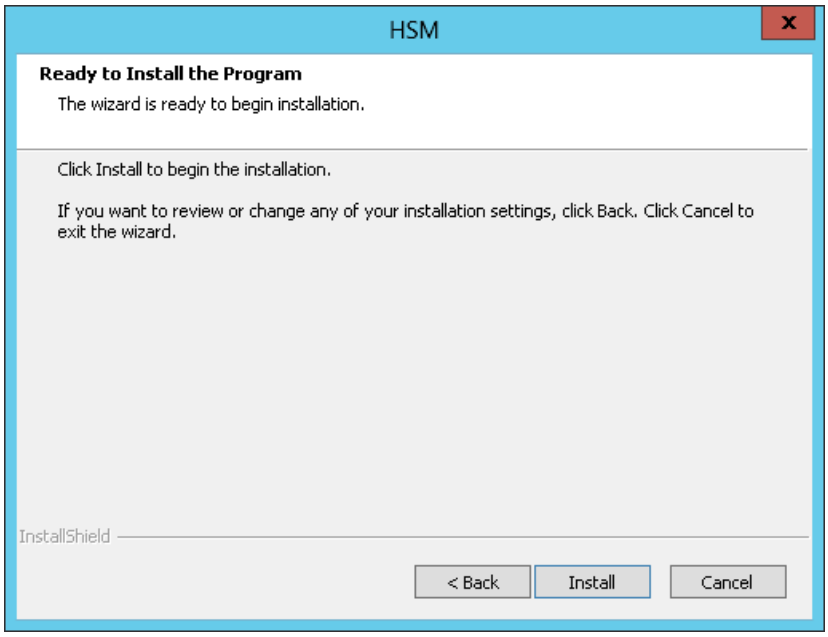
1. Run **HSM Setup**.
2. On the **Welcome** page click **Next**.
3. On the **Logon Information** page specify the user account under which the application will be running. It must be in the format DOMAIN\Username.



4. If the Windows Firewall is on and enabled, it is necessary to allow HSM components to communicate through Windows Firewall. The components (COM+ Network access and HSM services) will be added to the Windows Firewall Exception list. Click **Next**, then **Install**.



5. Upon successful installation of HSM, click **Finish** to exit the wizard.



Configuring HSM

When installation of HSM is complete, the **Configuration** tool opens. Here you need to configure HSM, i.e. you need to specify:

- database you will be using;
- schema; and
- media store where files will be archived.

NOTE: In the **Configuration** tool you can see also tabs of other Archive Manager products, if they are installed on the machine. In this manual we will describe the configuration just for the HSM tab.

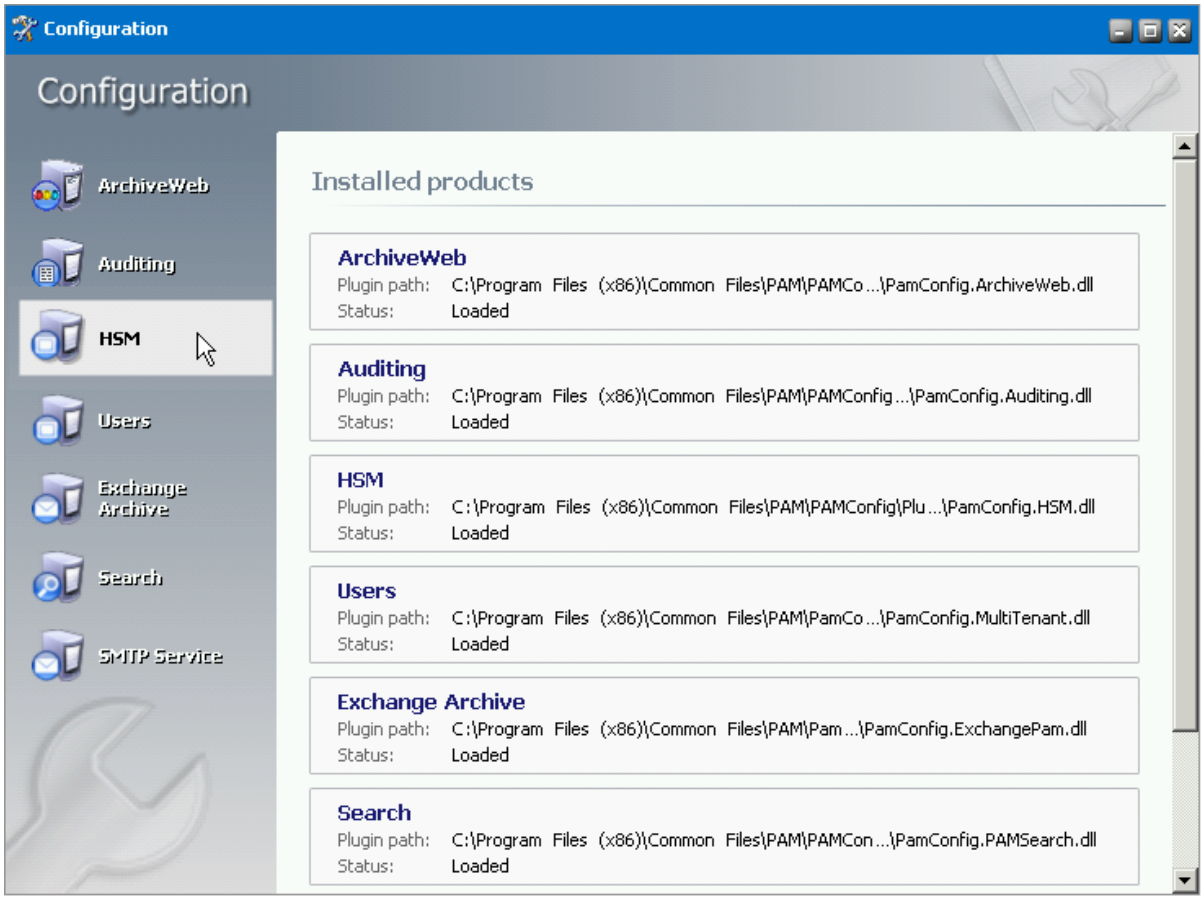
NOTE: Whenever you change the database password, use the **Configure** button of the **Configuration** tool to configure the database connection string. It is not enough to update the database objects in this case, since it is not updating the connection parameters.

When updating HSM from one version to another you **must NOT change the following values in the Configuration** tool:

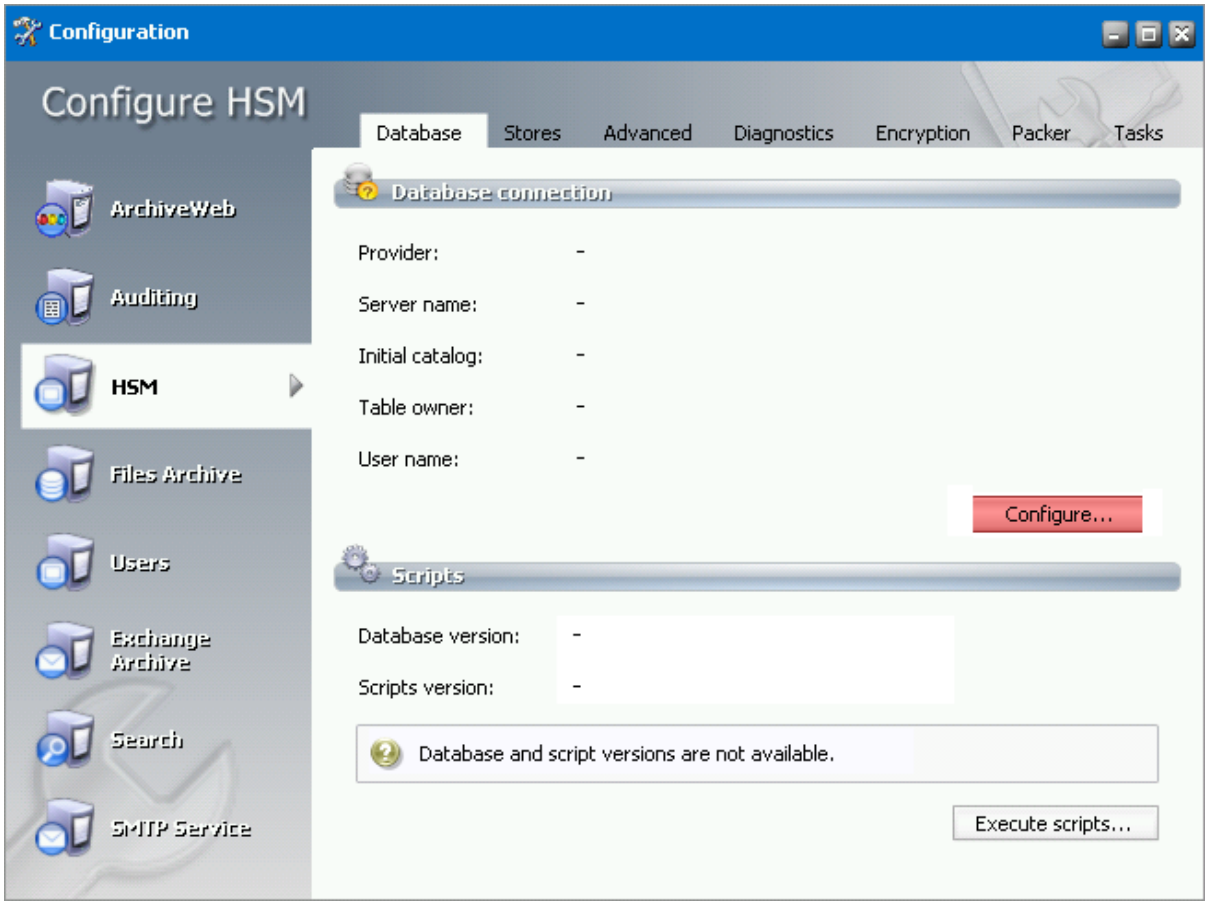
1. **Initial Catalog**: this is the default Database where the system is writing and reading from. This name should never be changed, unless you do not specifically restore all the prior archived data back and decide to start all over with a fresh new database for the product. If by mistake another database is used the old archived data is no longer reachable.
2. **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 2012 or higher, the Table Owner is the SCHEMA NAME of the database.
3. **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

To configure the HSM, follow these steps:

1. In the initial **Configuration** window select the HSM tab in the left pane. (By default **Configuration** tool can be found under **C:\ Program Files (x86) \ Common Files \ PAM \ PAMConfig**.)

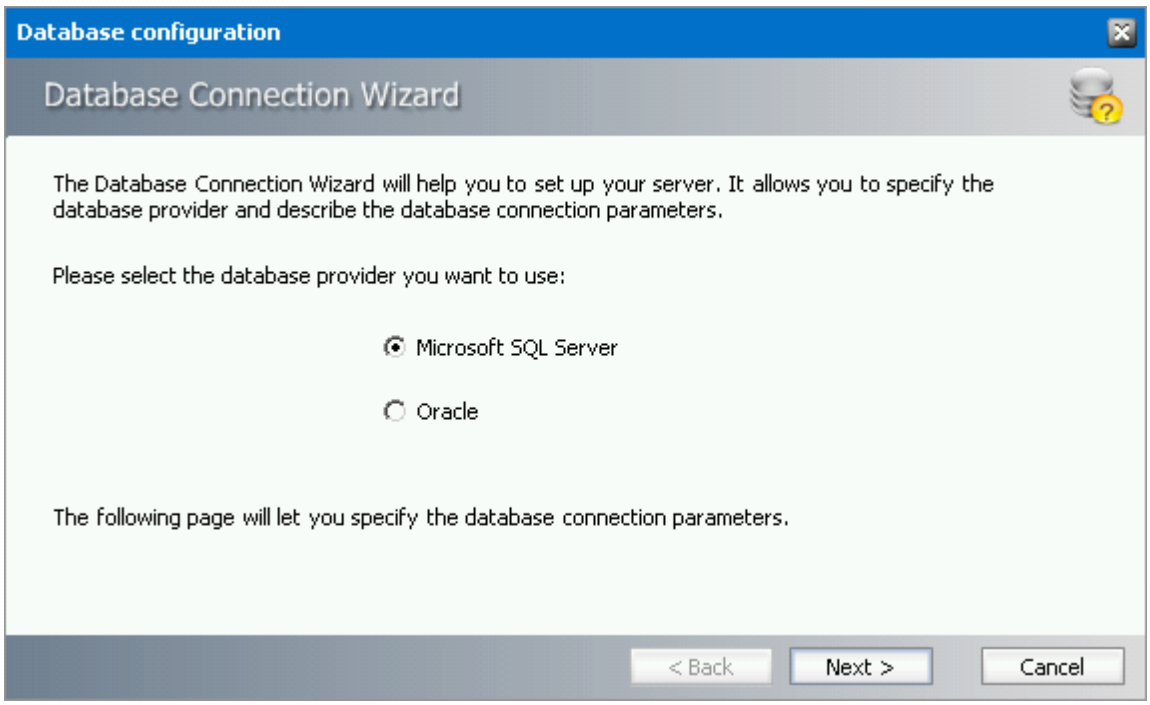


2. Click the **Configure** button to start the **Database Connection Wizard** and update the configuration settings.



3. In the case that you are working with an MS SQL database, select the **Microsoft SQL Server** option and then click **Next**.

   NOTE: For an Oracle database select the **Oracle** option.



4. On the next page please enter the requested data:

   - If you have selected **MICROSOFT SQL SERVER** in the previous window, fill in these fields:

     Server name (the name of your MS SQL server)

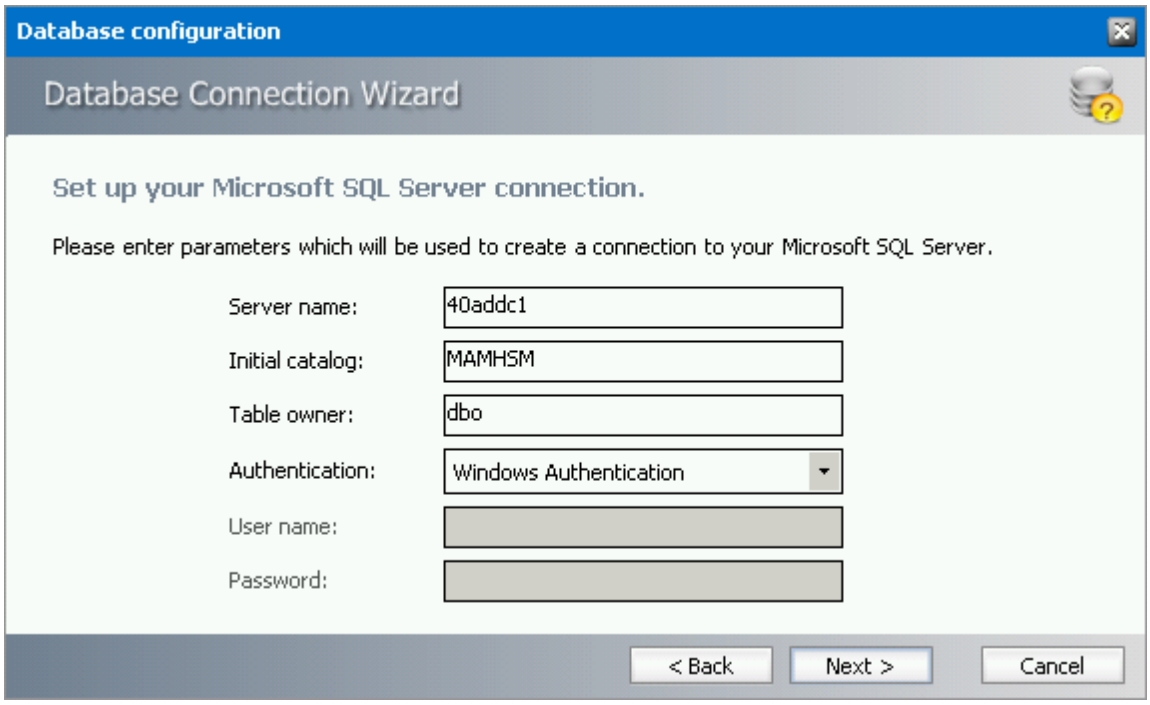
     Initial catalog (the name of the database for HSM)

     Table owner (the owner of the table or schema)

     Authentication (authentication type used for the database)

     User name (the database login name, if applicable)

     Password (enter the requested password, if applicable)



   - If you have selected **ORACLE** in the previous window, fill in these fields:

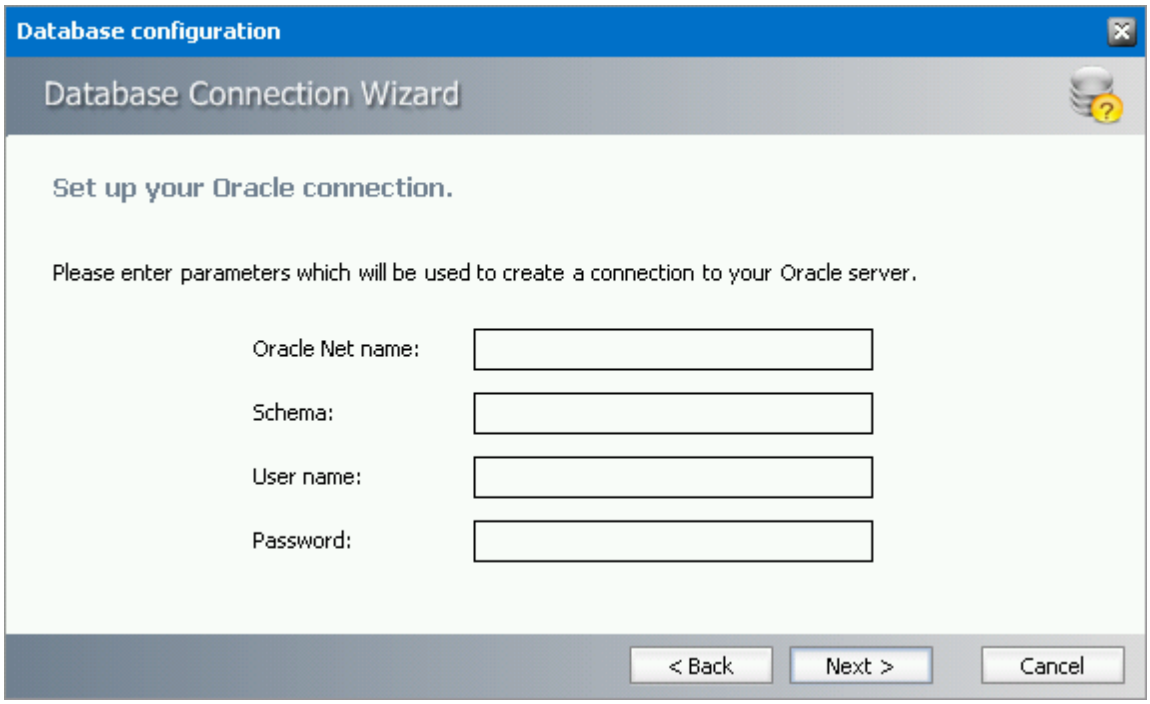
     ORACLE NET Name (ORACLE NET name, TNS name)

     Schema (the name of the schema where HSM tables will be created)

     User name (log-on user for the database with read and write rights to the table)

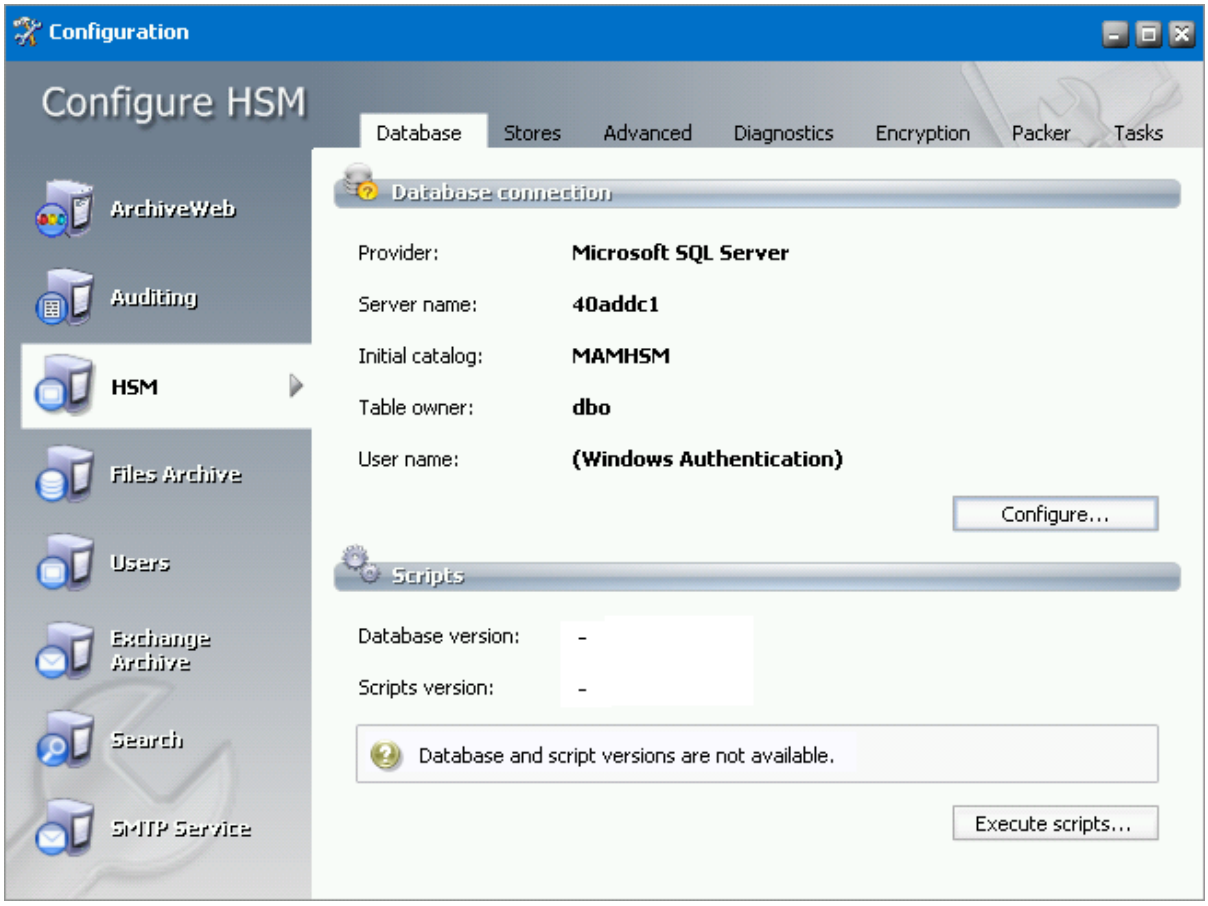
     Password (log-on user's password)

Afterwards, click **Next**.

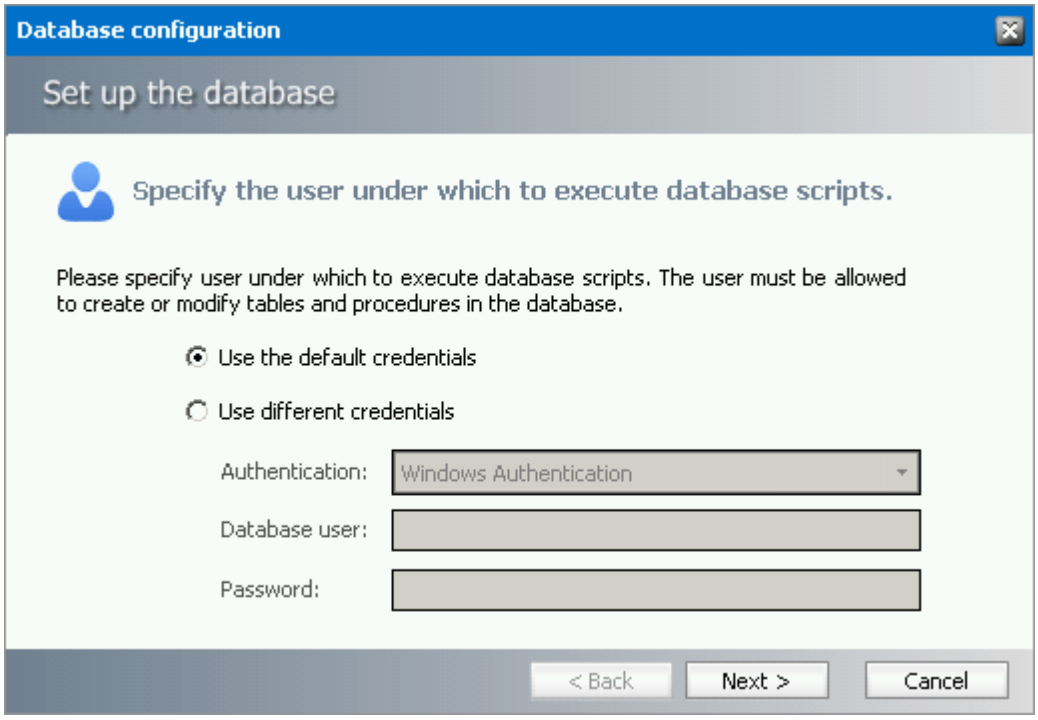


5. Click the **Finish** button. Next, you will have to run the database scripts.

   Back in the **Configuration** window on the **HSM** tab the data you have entered are now filled in. Run the scripts by clicking the **Run Scripts** button in the **Scripts** section.

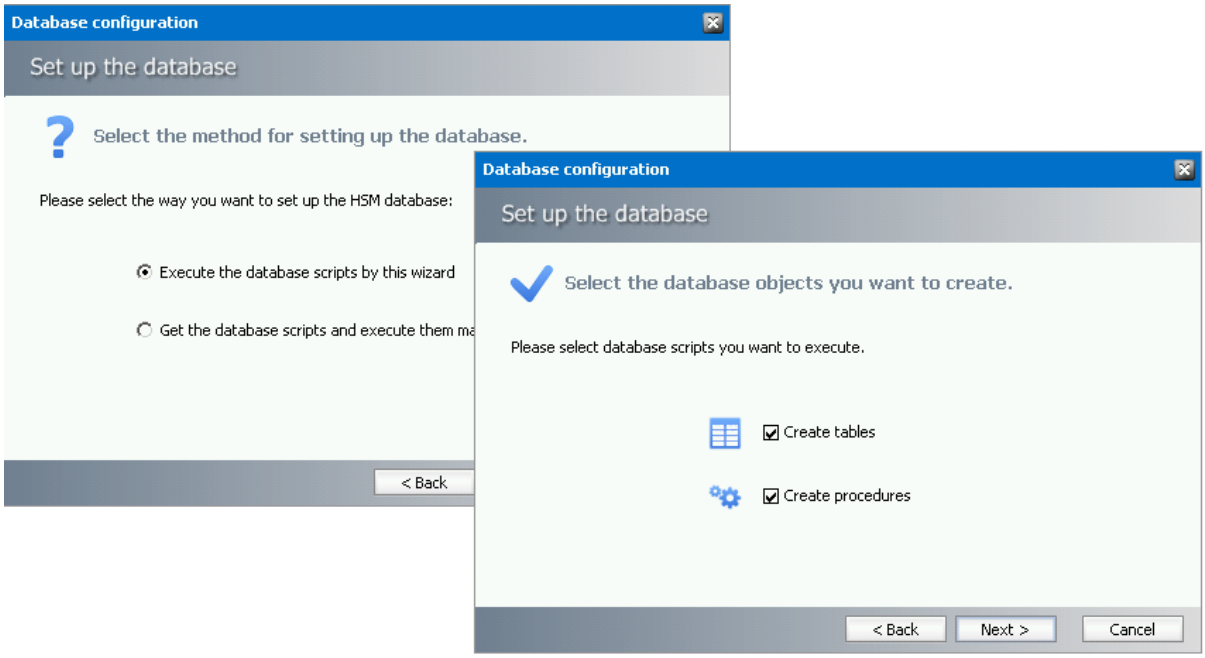


6. Now enter the database user under which the scripts will be run. If the **Use the default user credentials** option is checked, the user set in the database connection configuration part is used. If the **Use different credentials** option is selected, it is possible to choose the type of Authentication and other user's credentials. For the SQL Server Authentication specify the Database user and Password. Remember that the user must be allowed to create or modify tables and procedures in the database. Click **Next**.



7. Next choose the way to run the scripts. Either run them automatically (**Run database scripts by this wizard** option) or you can get the scripts and run them manually on your own by copying and running the script in a third party tool (SQL Manager, TOAD etc.)

   We have selected the 1st automatic option. After clicking **Nex**t and again **Next** a confirmation dialog displays. Click **OK**, then **Finish**.



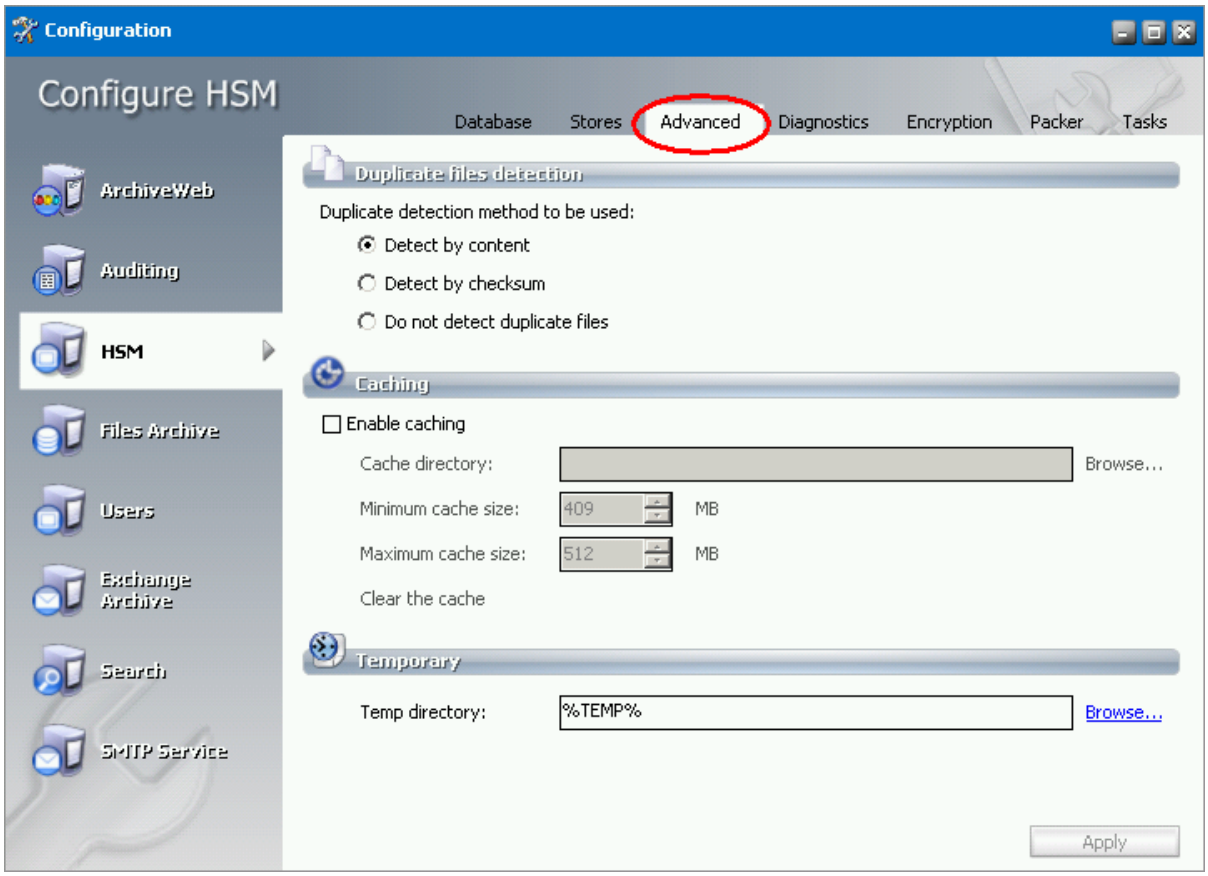
8. Back in the **Configuration** tool switch to the **Advanced** tab. The HSM system includes the Duplicate Files Detection service, it means that identical files are stored only once.

   In the **Duplicate files detection** section you may specify the duplicate detection method:

   a) Select the **Detect by content** option, should you wish to use the size, checksum and content for detection.

   b) Select the **Detect by checksum** option, should you wish to use the size and checksum for detection;

   c) Select **Do not detect duplicate files** option, should you wish to disable this detection



In the **Caching** part:

Use caching in case of slow storages (tape etc.). HSM will cache the recently used files to speed up the retrieving process.

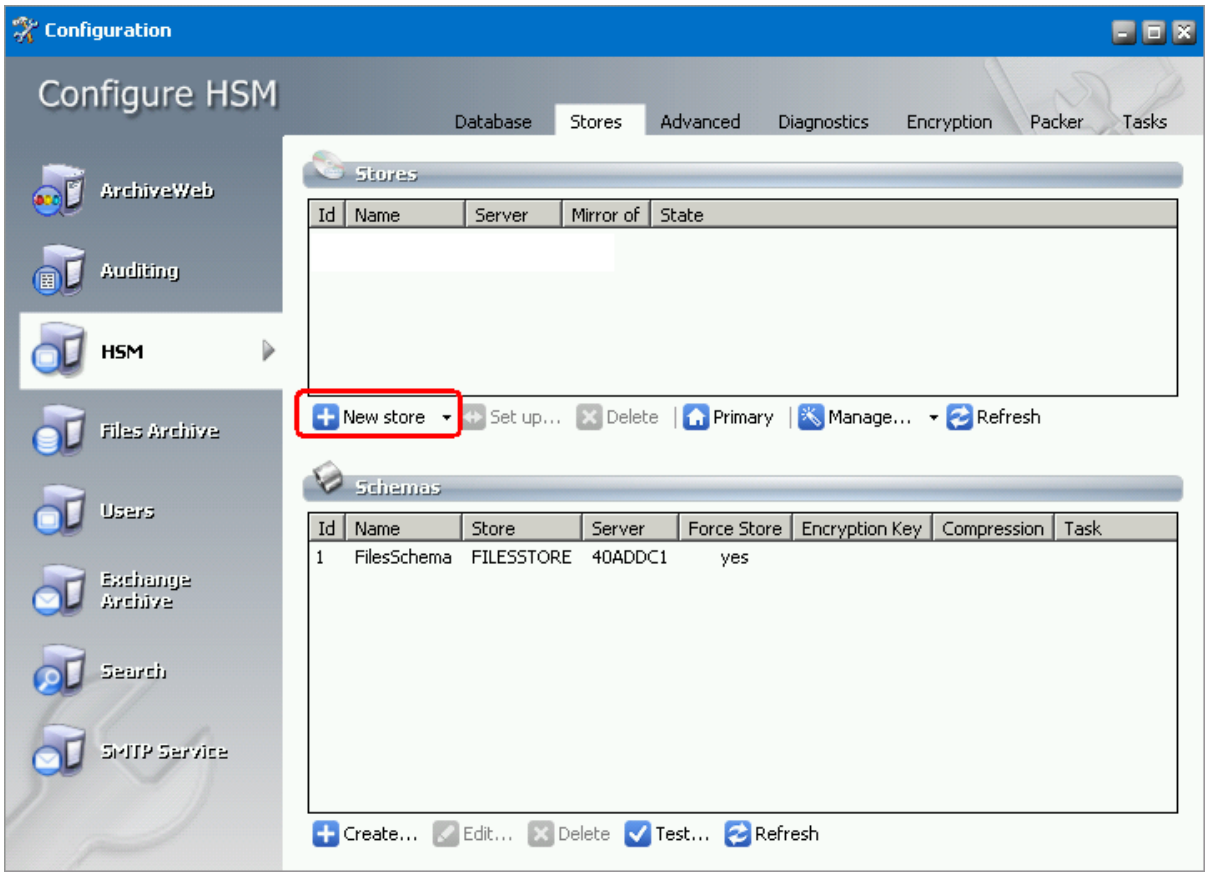
If **Enable caching** is checked, HSM will copy all retrieved files to an HSM internal cache. To set the **Cache directory** (which should be a local hard disk), use the **Browse** button next to the respective text box. If you have a cluster, the HSM will know that each installation has its own path.

Set the **Minimum cache size** and **Maximum cache size** as well. The **Minimum size** should be about 80% of the cache size. If the cache is full, HSM will delete files (the oldest first) until the cache reaches the "minimum size".

NOTE: To set which specific store should be cached, go to *Stores* tab. Then select the store and click *Manage* to edit its configuration.

The HSM stores temporary files created during duplication detection, compression etc. in temporary directory. Its location can be set in **Temp directory** text box. Usage of environment variables is allowed in this box (e.g. %TEMP% denotes the temp folder of the currently logged on user).

9. Now click on the **Stores** tab. You need to create a MediaStore and you need to specify a schema here.



To create a MediaStore, see the next part: "Creating a MediaStore".

To specify a schema, see the part "Specifying a Schema".

If you already have created a store, e.g. on a remote server, add it to the *Stores* list by clicking the downward arrow next to the **New store** button and selecting **Attach**.

NOTE: You must have at least **1 store** and at least **1 schema** available in order to archive with Archive Manager. For each HSM store (MediaStore) assign a schema. Assigning

more than one schema for the same HSM store where Archive Manager will be archiving files is also supported.

Creating a MediaStore

In this section you will be shown how to create a MediaStore and how to configure it.

When running installation for the first time you need to create a MediaStore (or you must have one available) and configure it. Later, when running it again, you may modify an existing MediaStore, or delete it, or even connect to a remote computer if a MediaStore is placed there.

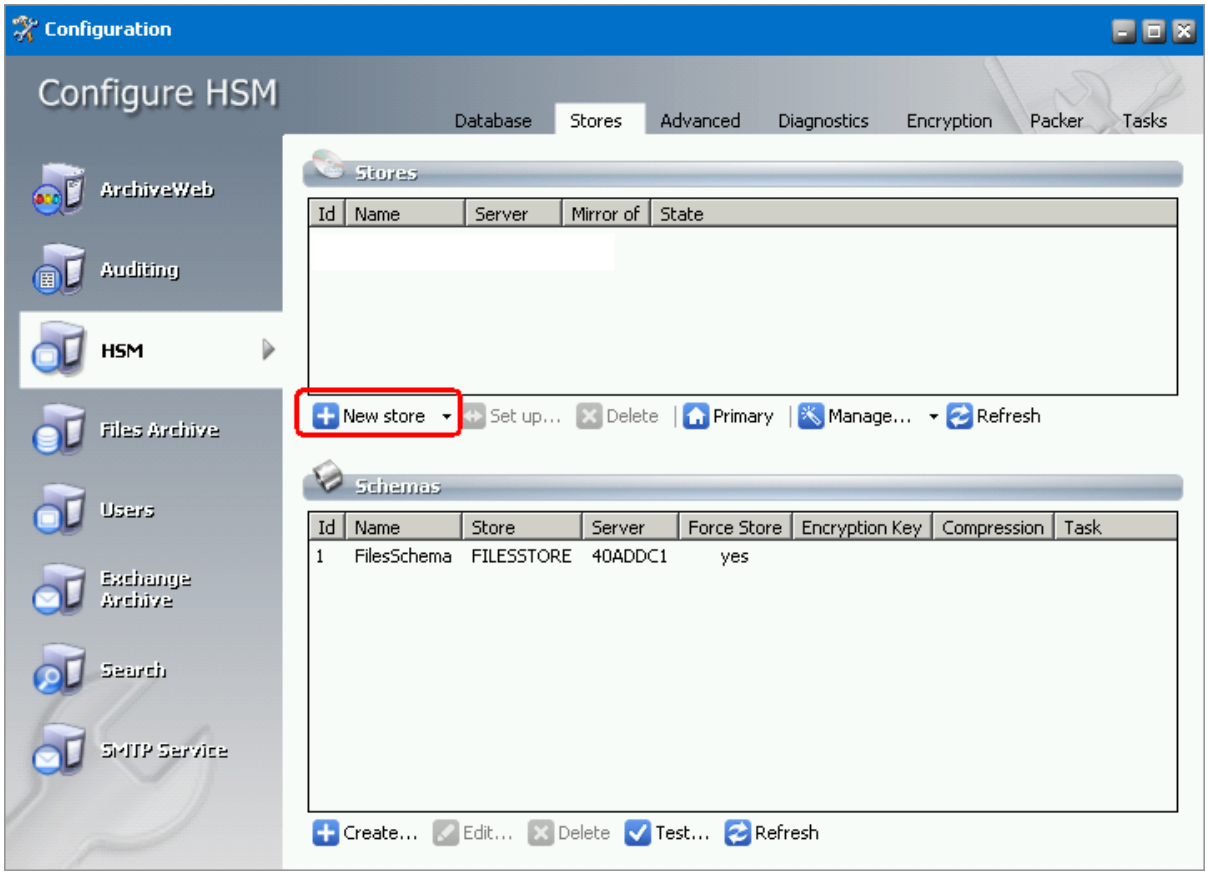
To create a MediaStore you basically need the following information: the UNC-path to a jukebox (AMASS, PEGASUS, or POINT) which is prepared for usage, and a second path if, for security reasons, you want the files to be archived also at some other location (i.e. under some other path as well).

RECOMMENDATION: The following lines describe the process for **Jukebox, Hard disk, Network** option. However, provided that you do not need directories with a specific size (e.g. 5 GB) and you have a Hard disk or RAID-system we recommend **Simple Path** store-type. This kind of store is faster and outperforms all other stores under the same circumstances (same hardware, same path) (see the following section "*Simple Path MediaStore*").

Jukebox, Hard disk, Network Media Store

To create a Jukebox, Hard disk and Network MediaStore, do as follows:

1. In the **Configuration** tool on the **HSM** / **Stores** tab click the **New Store** button to open the *MediaStore Administration* wizard.



NOTE: When there are already some stores created, buttons under the *Stores* list view can be used to administer them:

New Store – use to create a new store (as described further in this section); it is also possible to attach already created store – to do so, click the downward arrow and select *Attach*

Set up – setup store mirroring

Delete – deletes the selected store if no schema is assigned to it

Primary – displays only primary stores, i.e. stores that are not a mirror for any other store

Refresh – refreshes the list view

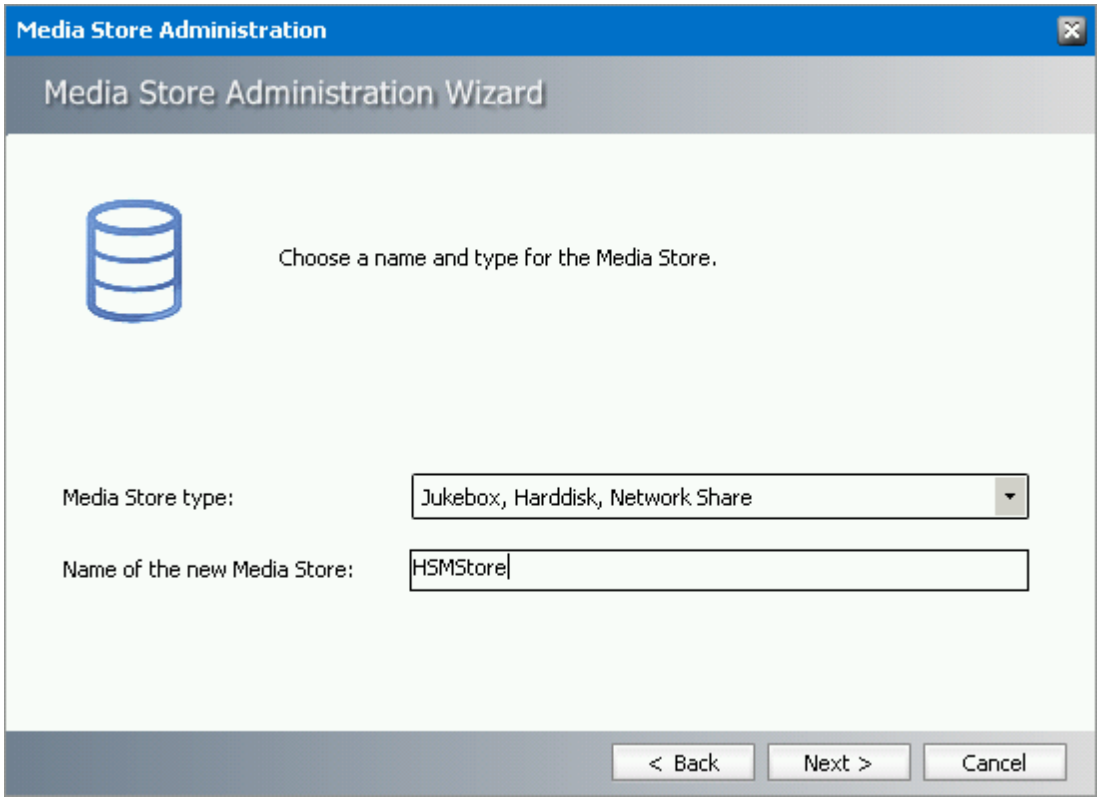
Manage – opens configuration wizard for the selected store; you can also start or stop created stores by selecting it and clicking the Manage down arrow / *Manage service state*

2. To configure the MediaStore, select the desired **MediaStore type** in the dropdown.

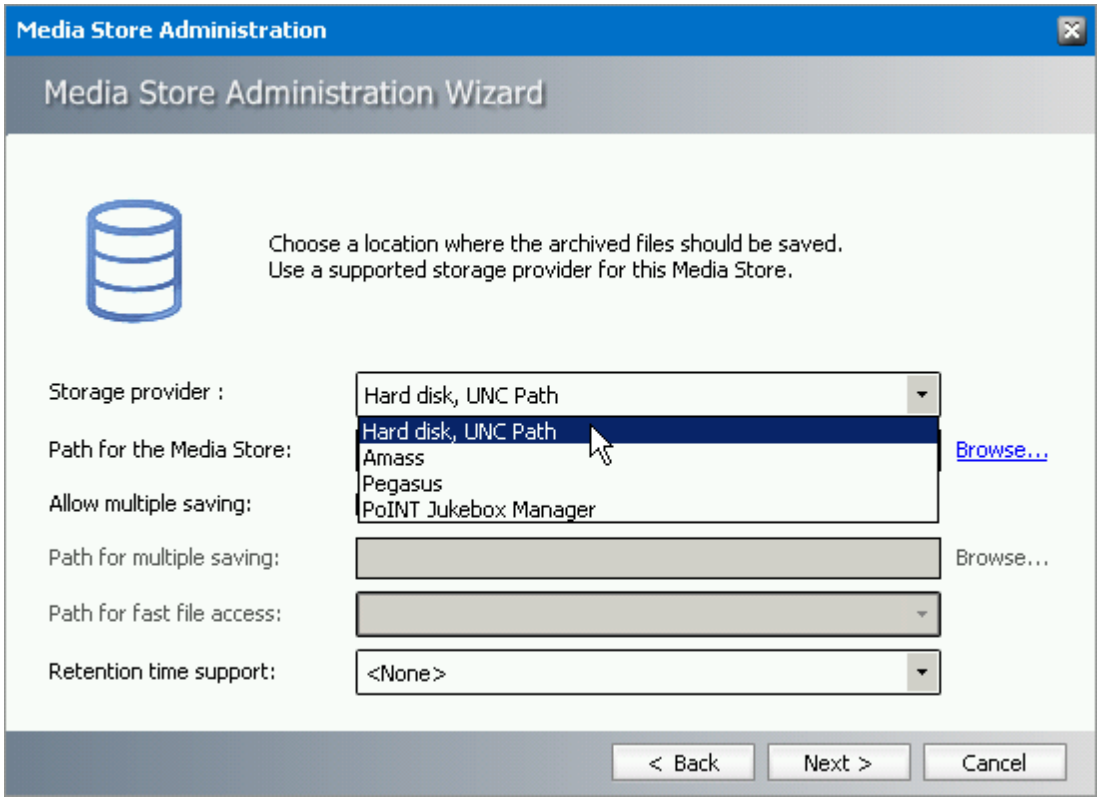
NOTE: We will describe the process for the **Jukebox, Harddisk, Network** option. However, if you have a harddisk or raid-system, and you do not need directories with a

specific size (e.g 5 GB) always use **Simple Path** store-type (see “Simple Path MediaStore” section further in this manual).

Then enter a name for your new MediaStore in the **Name of the new MediaStore** text box. Click **Next**.

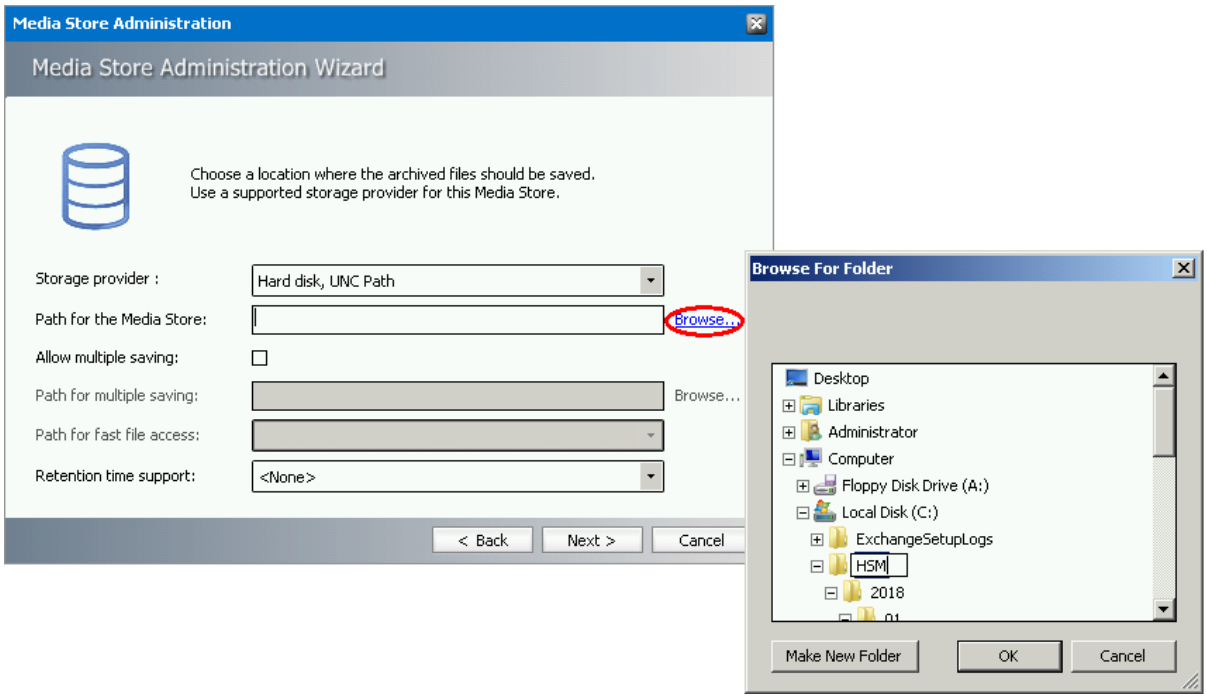


3. In the **Storage Provider** drop-down list select either **Hard disk or UNC path** (in the case that your store will be placed on a hard-disk drive or share) or the appropriate storage provider, i.e. the manufacturer of your jukebox software: **Amass**, **Pegasus**, or **PoINT Jukebox Manager**.



4. Click on the browse button next to the Path of the MediaStore box choose a location of the desired MediaStore. Click OK.

   NOTE: To create a new folder, use the **Make new folder** button. Enter the name for this new folder, e.g. HSM and click **OK**.



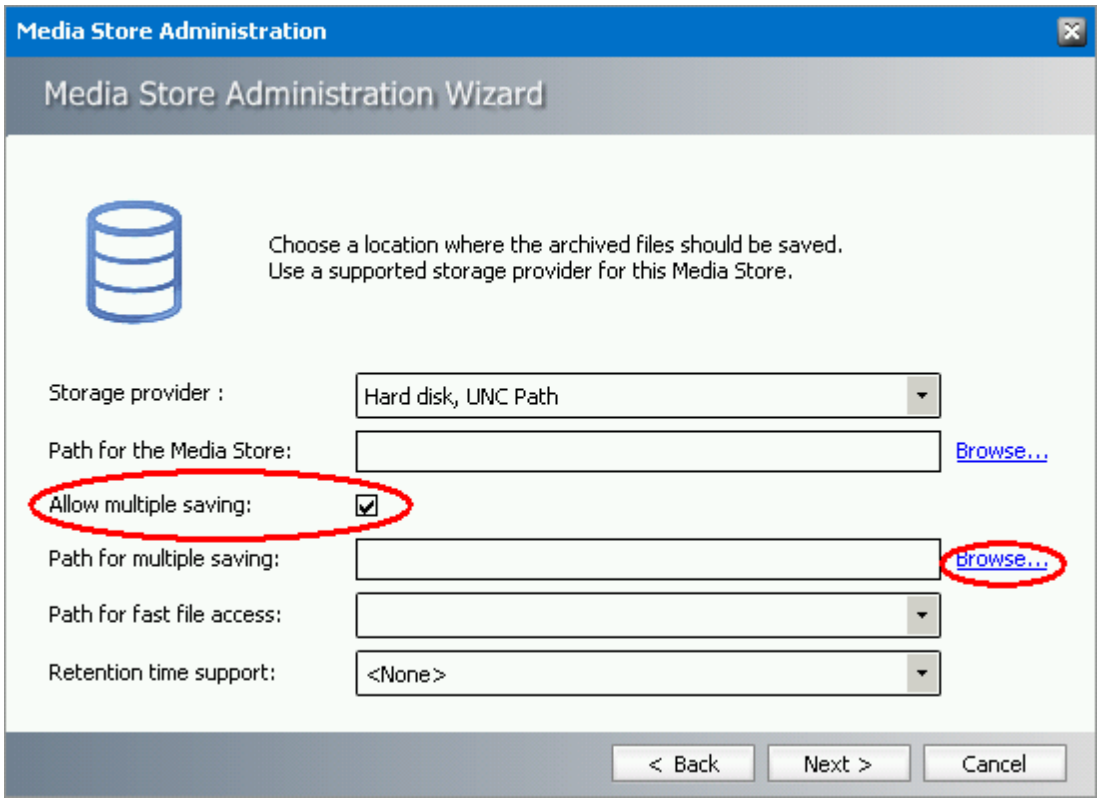
5. Should you wish to archive files simultaneously to some other location as well, select the **Activate multiple saving** check box. Use the **Browse** button, similarly as above, to specify a second path.

   The files will be archived to this second location, too.

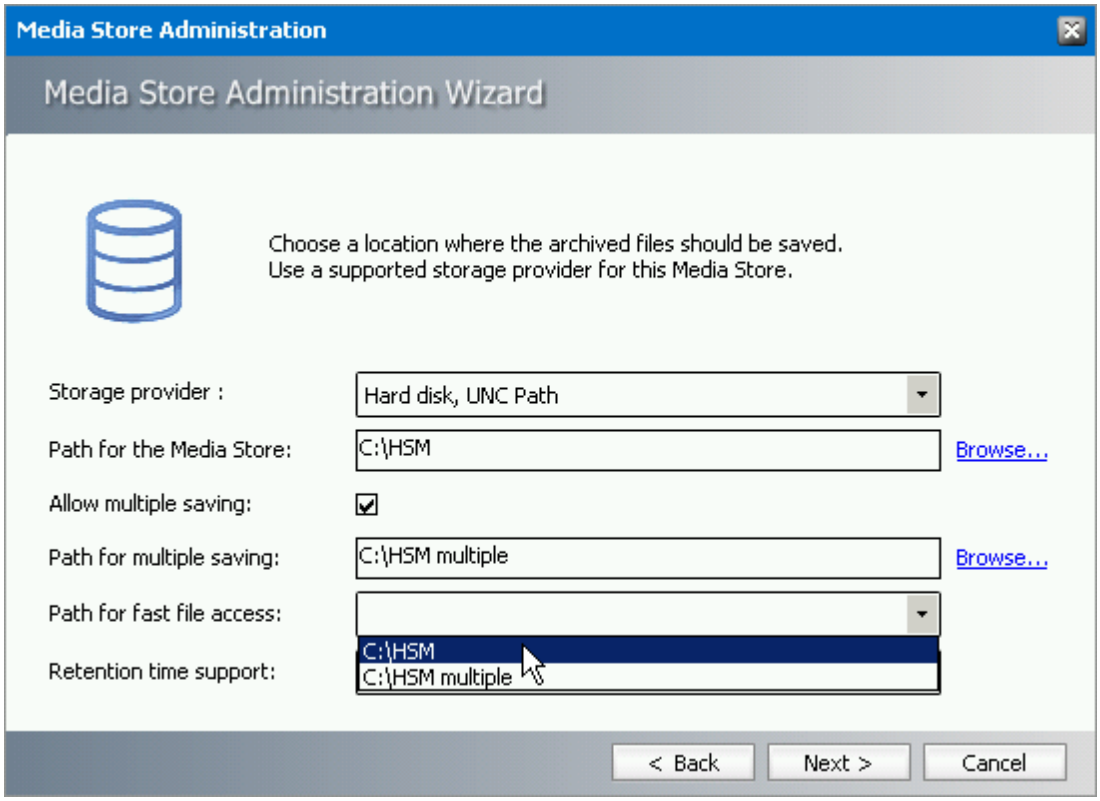
   NOTE: The second path can be anything that is reachable by a drive-letter or a network share, something accessible with Windows Explorer.

   In normal usage the first path is a slow MediaStore (e.g. Pegasus Jukebox), and the second path is a large SAN (e.g. local RAID or Harddisk). For fast access you should use SAN because it is much faster.

   WARNING: If archiving to one path fails, file store operation will result in error.



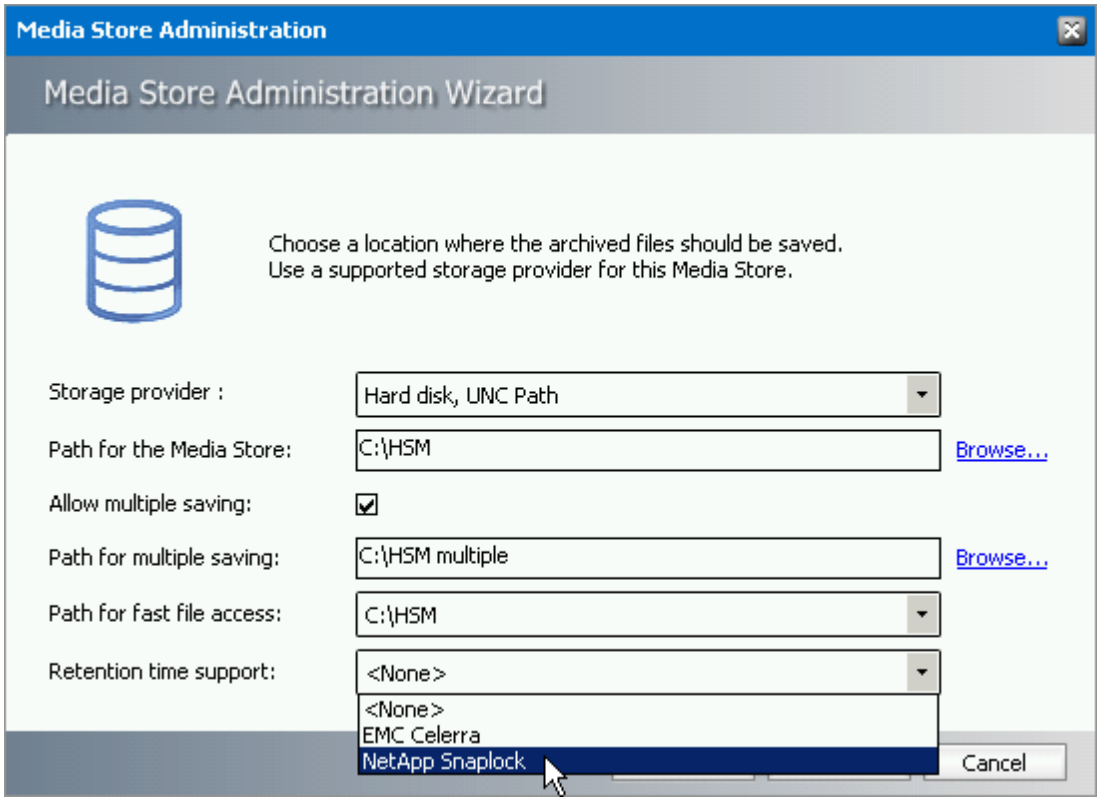
6. In case that you activated multiple saving, click on the down arrow next to the **Path of the fast file access** path drop-down list and select the faster access path.



7. In the **Retention Time support** drop-down box select the **NetApp SnapLock** option if you are using NetApp and want to use SnapLock to secure the compliancy with law regulations regarding archiving of electronic documents. (e.g. HIPAA, OFRS, COSO etc.)

   In case you are using EMC Celerra and you wish to use retention times for your archived files, select **EMC Celerra**.

   Click **Next**.



8. In the case that you activated multiple saving the following window gets displayed. Here you may configure multi-storing.

   The **Multiple Saving** section:

   Should you select the **From the medium with number** check box, then you may choose from which numbered medium multiple saving was activated.

   Should you select the **For the last media** check box, then you may enter a number which will specify up to which media multiple saving would be done.

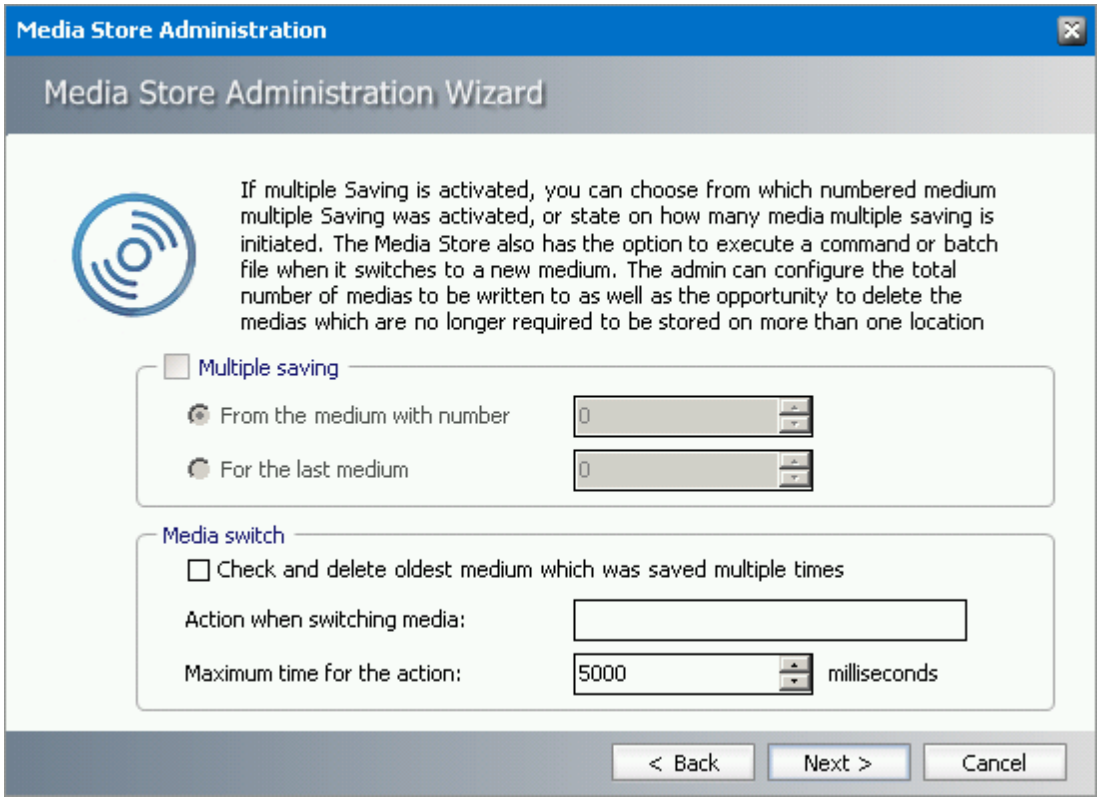
   The **Media Switch** section:

   Should you select the **Check and delete oldest medium which was saved multiple times** check box the system will check for media which are no longer required to be stored on more than one location and deletes the redundant copies.

   In the **Action when switching media** text box you may enter a command or a batch file that will be run when switching between media.

   In the **Maximum time for the action (ms)** text box specify a maximum time frame that you want to set for the action.

   Then click **Next**.



9. On the following page you need to configure media names. You also need to specify the total number of media in this MediaStore to be used by Archive Manager product.

   In the **Create folder names using** down-drop box select whether HSM folders names should be created in lowercase only, uppercase only or standard.

   If you select the **Create file and folder-names using 8.3 convention** check box then the file-name will be truncated to 8 characters and extension to 3 characters, provided that the underlying system doesn't support long filenames.

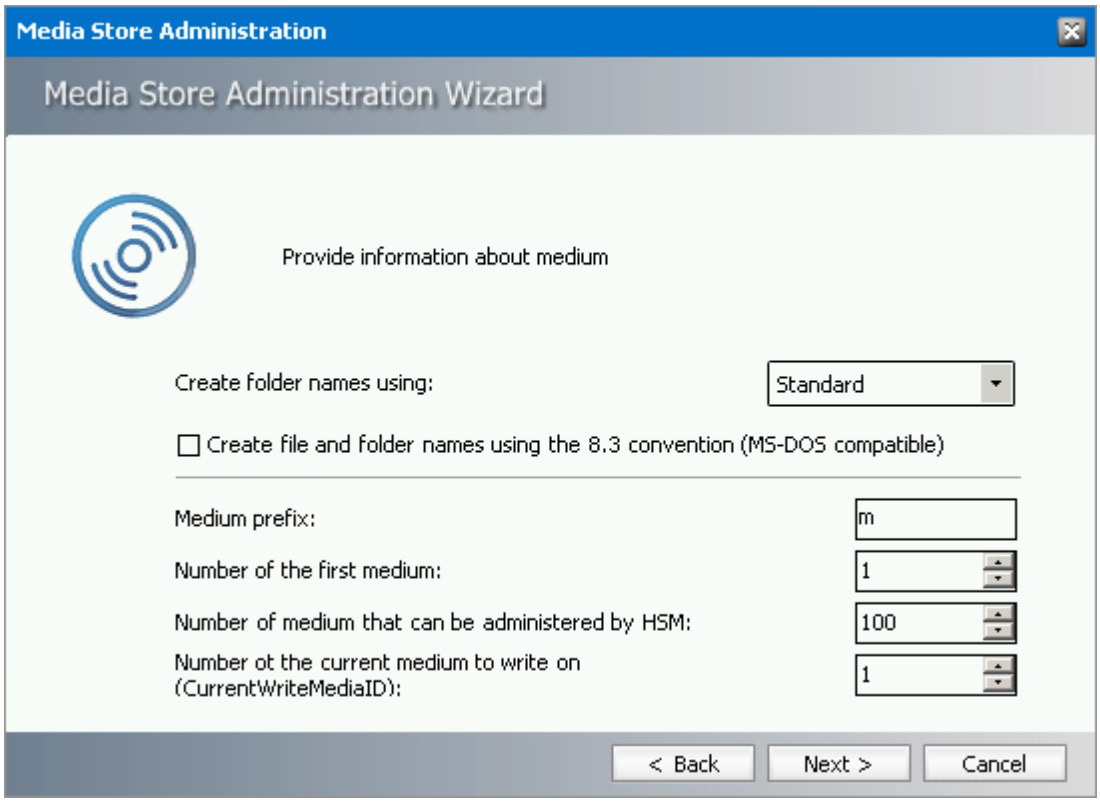
   To specify a prefix for the desired MediaStore use the **MediaPrefix** text box. You may enter 2 alphanumerical characters. Those characters will be located in front of each of the media along with the respective media number. In our example we chose LS as the media-prefix (as local store), so the name of one of the media would be LS000001.

   In the **Number of the first medium** text box you may specify a number that will be assigned to the first medium.

   In the **Number of media that can be administered by HSM** text box you need to specify the number of media to be administered by Archive Manager. For instance, if there are 20 media in a Jukebox, then enter 20.

   In the **Number of current media to write on (CurrentWriteMediaID)** text box you may specify the number of the medium that will be used as the first one for archiving.

   Click **Next**.



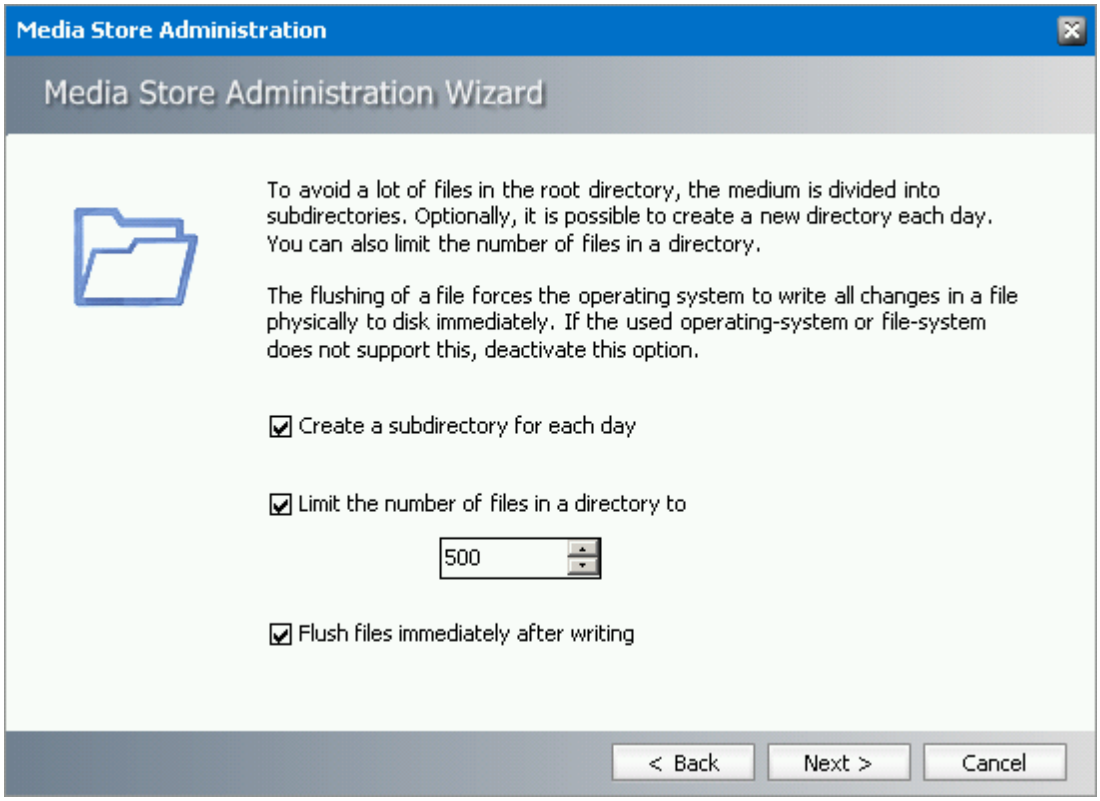
10. On the following page you may specify whether to create a directory for each day.

    It is recommended to select the **Create a sub directory for each day** check-box to create a directory for each day (an optimal condition). Subdirectories are being created with the path 000001, 000002, and so on. This is necessary for performance reasons, the more files a directory contains the longer the search for a file can take.

    By selecting the **Limit the number of files in directory to** check-box you may even limit the number of files per directory. Simply enter the appropriate data in the text field.

    Select the **Flush files immediately after writing** check box. Normally, all file-systems support flushing of files. Disable the option only if you have problems with storing files.

    Click **Next**.



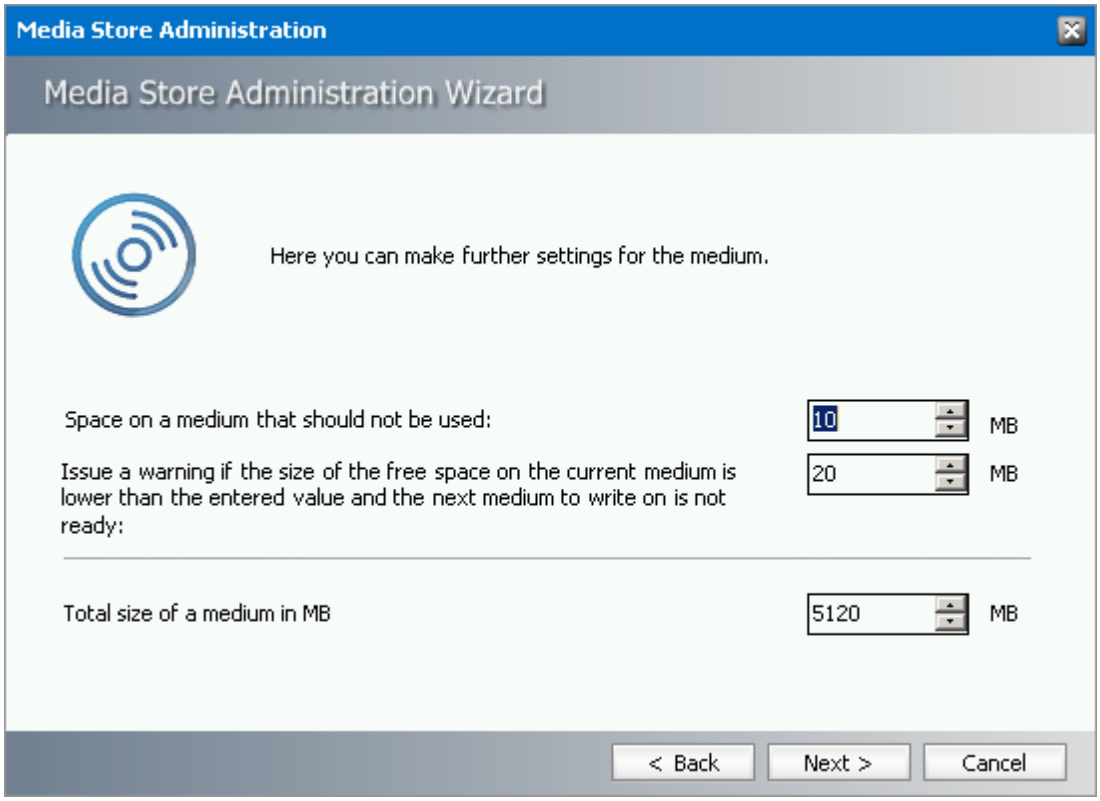
11. On this page you need to specify further settings for the used medium, as well as the total size of the medium.

    To set a storage space not to be used on a medium, enter the desired value in the **Space on a media that should not be used** text box. This value is defined in MB.

    Besides, you may set a value which refers to a warning message. As soon as free storage space is lower than the value specified in the **Issue a warning if the size of the free space on the current medium is lower than the entered value and the next medium to write on is not ready** text box, you would get a warning message. This value is also in MB. When this value is reached the availability of a new medium is being checked. This value should comply with the approximate average daily amount of MB to archive, so that new medium can be searched in a timely manner.

    In the **Total size of media in MB** text box you need to enter the total size of a medium.

    Then click **Next**.



12. HSM needs to know when to start a new medium, as there is maximum medium size set. For this purpose it needs to recalculate the used space periodically. On this page you may choose how often the free space on a medium should be calculated. It can be set in accordance with the number of files, or file size, or simply in seconds. As soon as any of those values are met, the remaining storage space is recalculated.

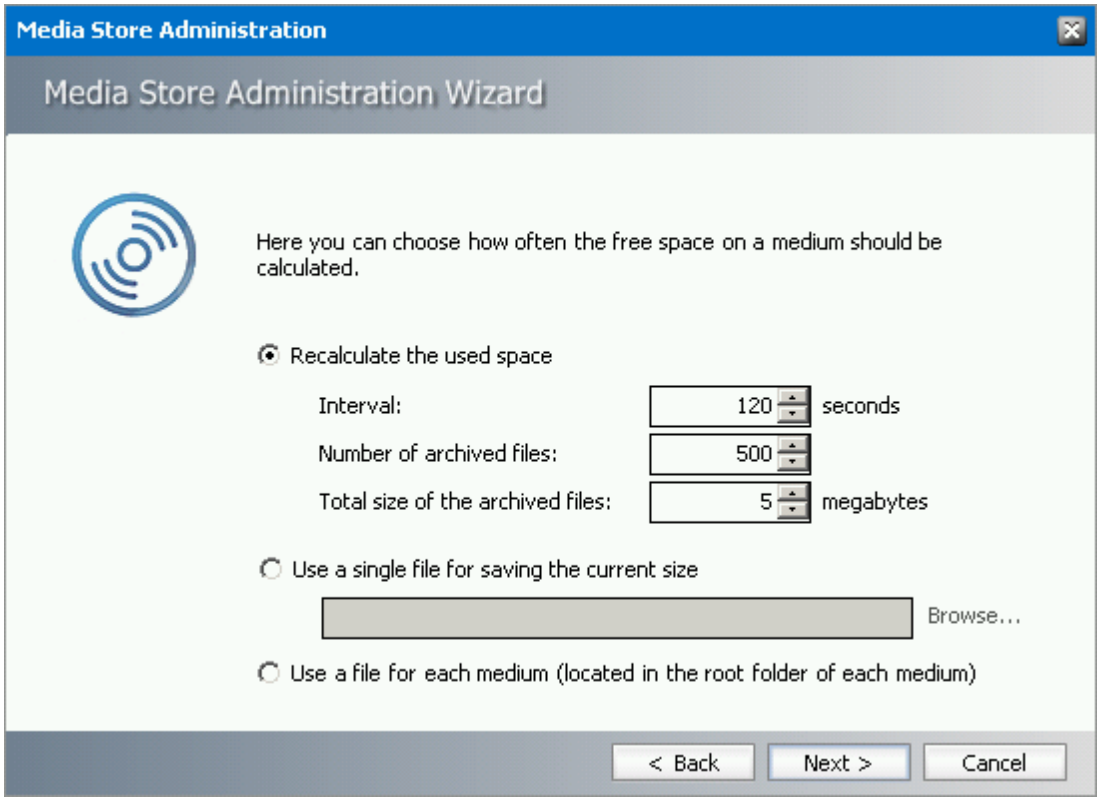
    To periodically recalculate the free space on the medium, simply enter a desired time span in the **Interval** text box.

    To recalculate the free space on a medium depending on the number of files that have been archived since the most recent calculation, simply enter the desired value in the **Number of archived files** text box.

    To recalculate the free space on a medium depending on the archived volume since the most recent calculation, simply enter the desired value in the **Total size of the archived files** text box. This value should be given in MB.

    If the user does not want to allow the HSM to recalculate the used space periodically (because it might be time-consuming operation), he can specify a file where the value of the used space on a medium will be saved. The file is updated each time a file is stored on the medium. Here he can decide whether to use a single file for this purpose for all media in the store – **Use a single file** check box - or create a separate file for each media – **Use a file for each media** check box.

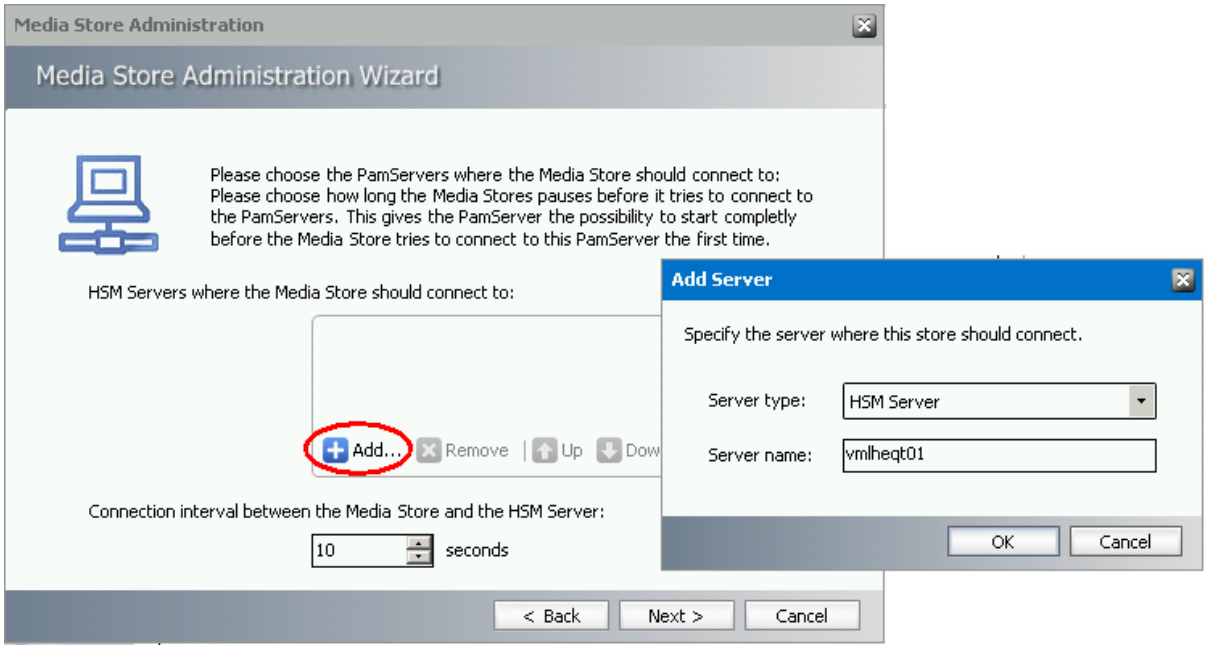
    Click **Next**.



13. On this page you need to specify where the MediaStore should connect to.

    Click the Add button to specify the HSM server.

    In the pop-up dialog set the **Server type** to “HSM Server” and enter the **Server name**.



The HSM Service contacts the MediaStore you specified in periodical intervals. Specify this interval in the **Connection interval between the MediaStore and the HSM Server in seconds** text box.

Click **Next**.

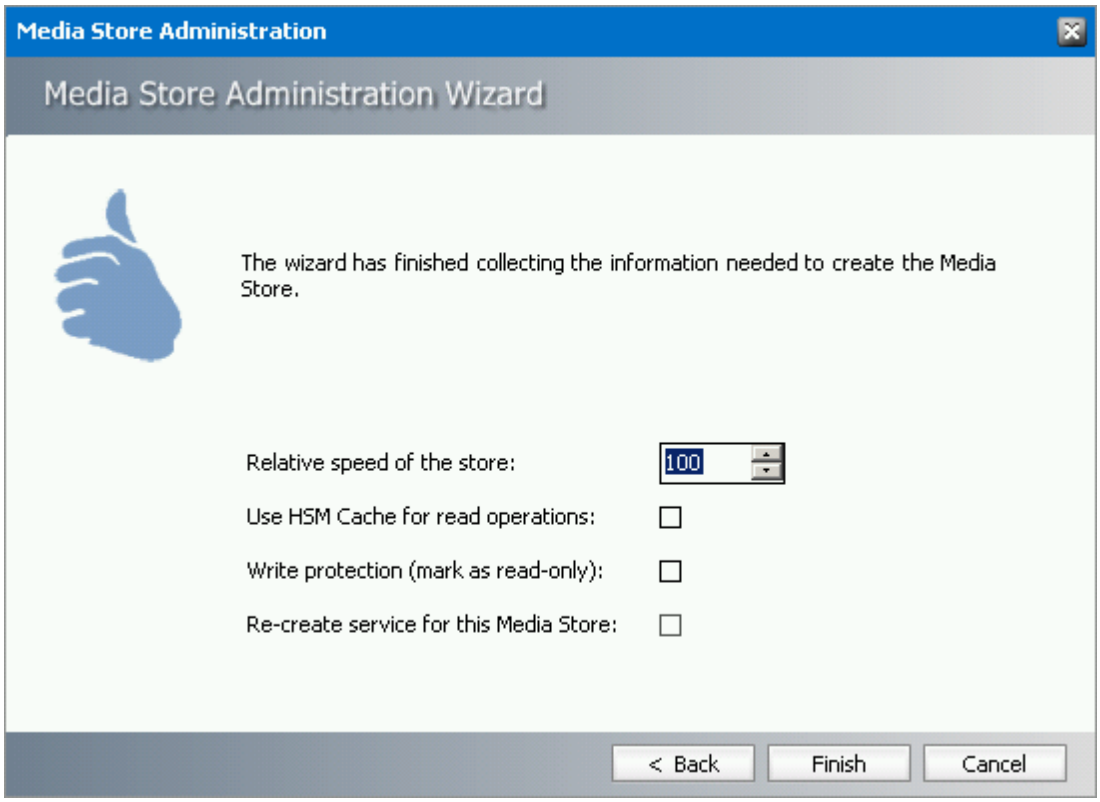
14. In the following dialog the **Relative Speed of the store** text box represents the relative speed of this store compared to other stores.

    If HSM should copy files into the cache when reading from this store, check **Use HSM Cache for read operations**.

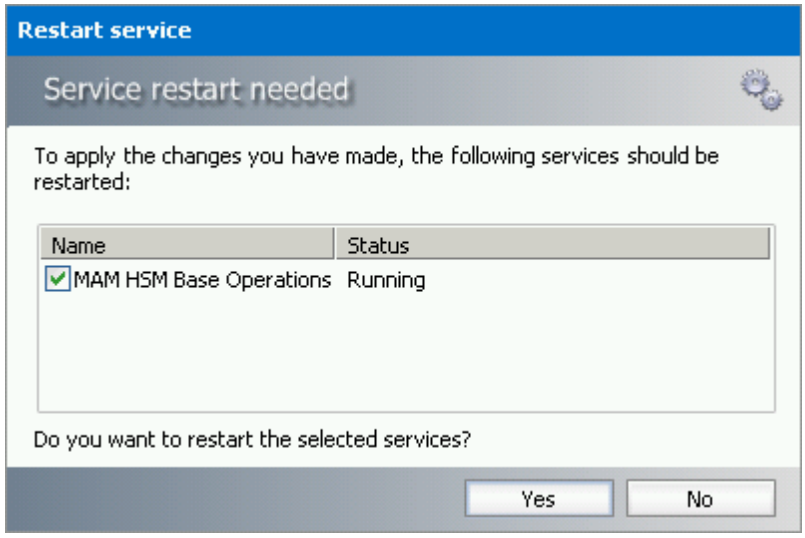
    If this media should be read-only, check **Write Protection** check box. (only supported for “Jukebox, Harddisk, Network” and “Simple Path”).

    If the **Re-create service for this media store** is checked, the store will be running in the background as a separate service. This option means that the MediaStore Administration Wizard should re-register the service for the administrated store. It is useful if the store service was deleted and the user wants to re-create it.

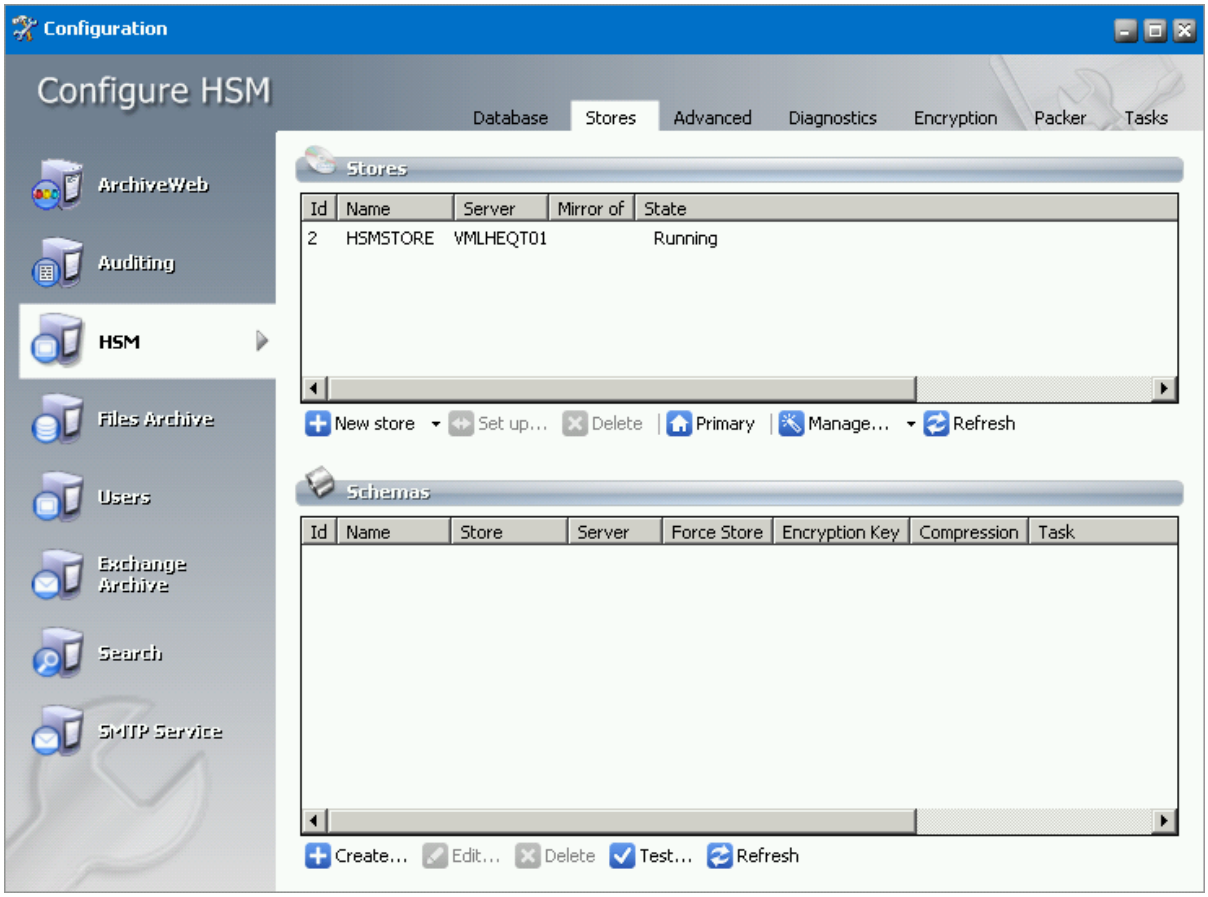
    Click **Finish**.



15. You will be asked to restart the service to apply the changes. To restart, click **Yes**.



16. Click on the **Finish** button to close the window.
17. Back in the **Configuration** tool the store you have created will be displayed in the Stores list view.



NOTE: Should the store display "*State – Stopped*" it needs to be started. To start a store, click **Manage** down arrow /Manage service state. Locate the desired store in the list and click **Start**.

NOTE: Should you be using several MediaStores, you need to repeat all steps as described in this section for each one of them.

Simple Path MediaStore

In this section will guide you through the process of creating **Simple Path** MediaStore. Should you have created your store already, (e.g. as described in the previous chapter) continue with the "Specifying a Schema" part of the manual.

When creating a MediaStore as described in the previous part "Creating a MediaStore" you can choose from several location for saving of archived files. We have described the process for **Jukebox, Hard disk, Network** option. However, provided that you do not need directories with a specific size (e.g. 5 GB) and you have a Hard disk or RAID-system we recommend **Simple Path** store-type.

This kind of store is faster and outperforms all other stores under the same circumstances (same hardware, same path).

Description:

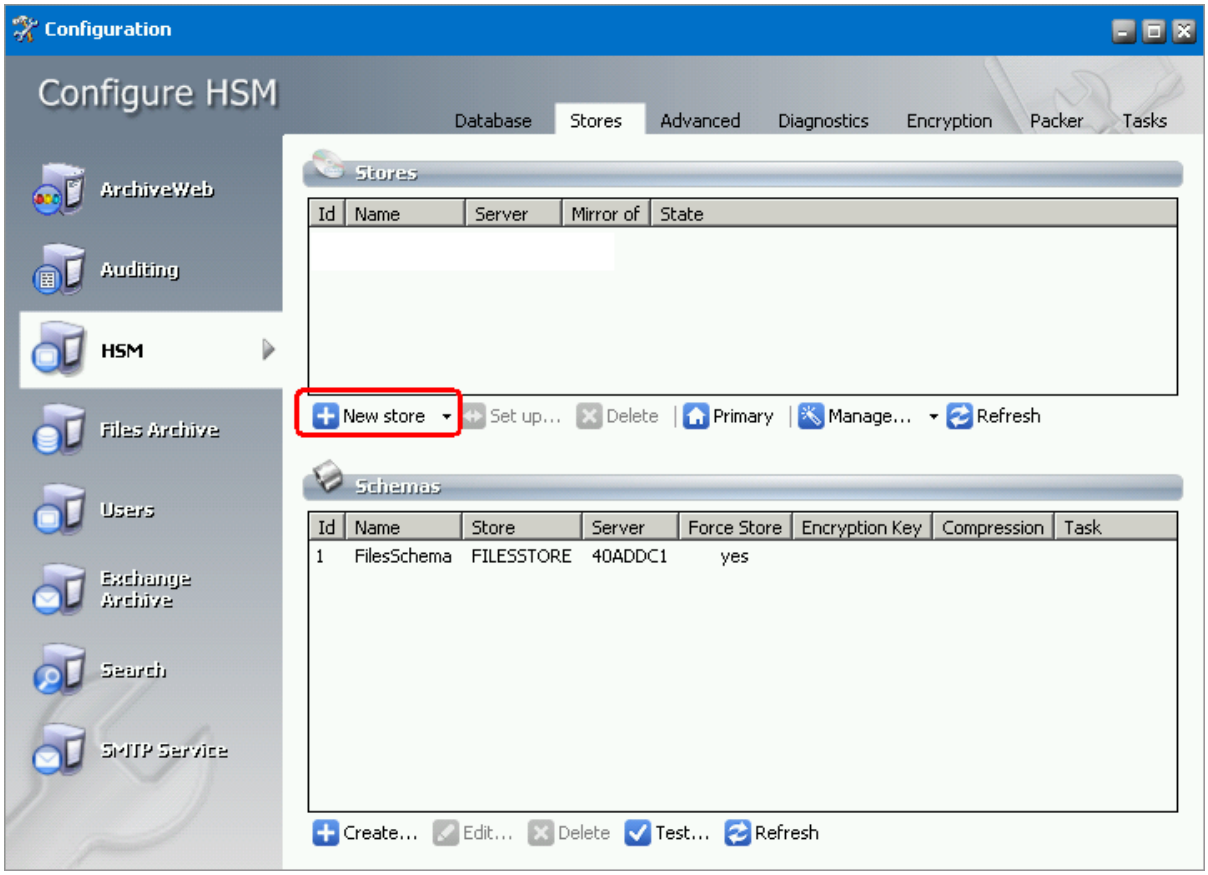
- It does not do size checking
- It writes files on any UNC path (e.g. Harddisk, Network-Share)
- Files are stored in subdirectories (there are no "medias" with a specific size)
  <RootPath>\<Year>\<Month>\<Day>\<Hour>\<counter>\Filename.txt
  e.g. e.g. D:\HsmStore\2007\04\26\18\000\ 4_000000f4.tif

NOTE: If you need to access a share you have to allow the computer account (Local System) to access a share or run PamHsmTSv with a special user.

To create a MediaStore – **Simple Path** type, do as follows:

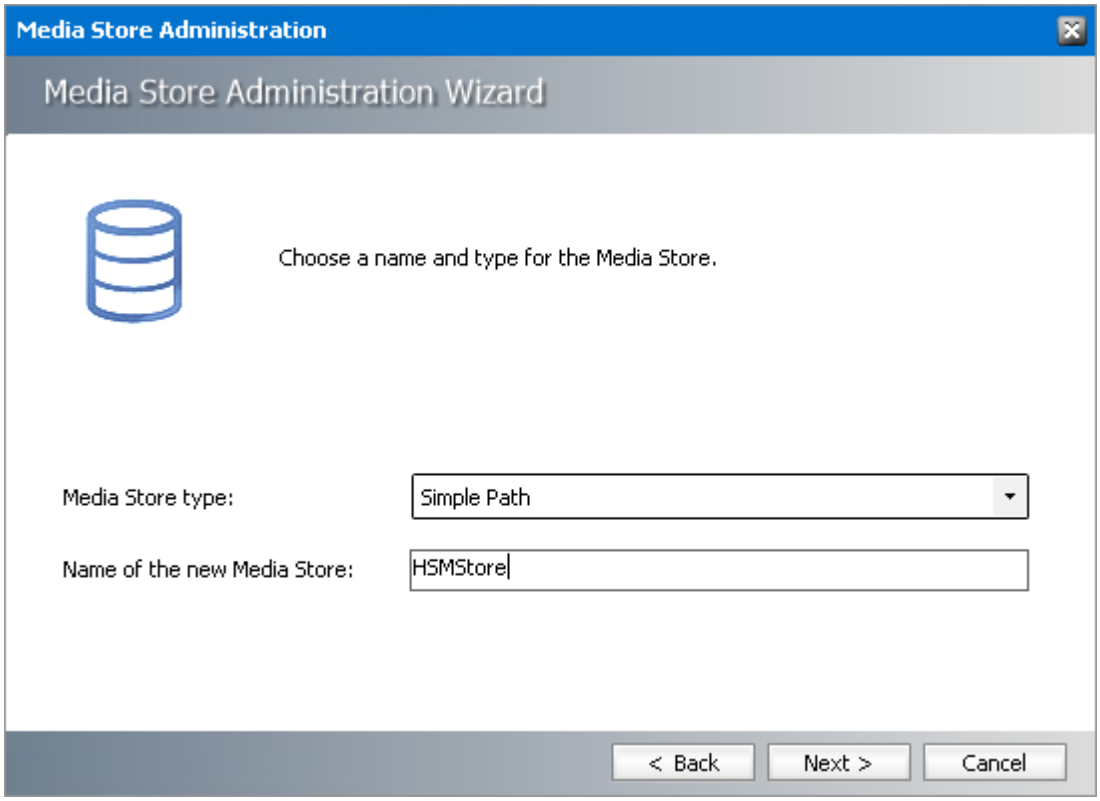
1. In the **Configuration** tool on the **HSM** / **Stores** tab click the **New Store** button to open the *MediaStore Administration* wizard.

   NOTE: By default **Configuration** tool can be found under **C:\ Program Files (x86) \ Common Files \ PAM \ PAMConfig**.



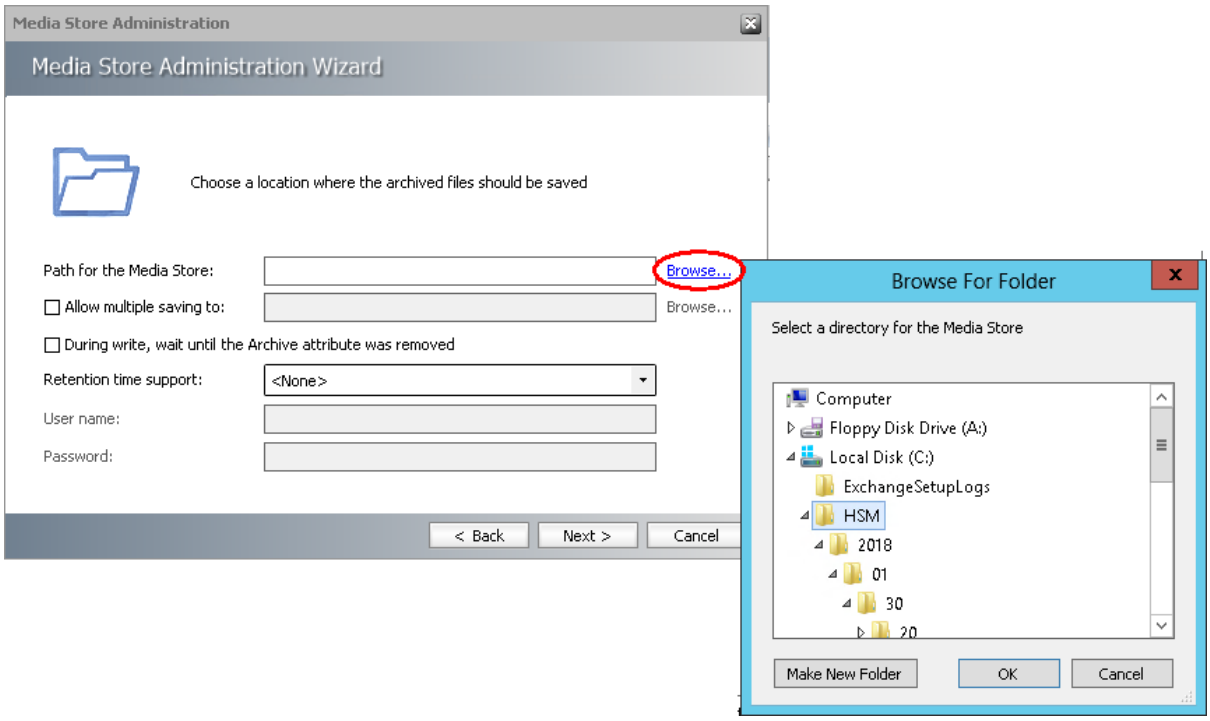
2. To configure the MediaStore, select the **Simple Path** option in the dropdown.

   Then enter a name for your new MediaStore in the **Name of the new MediaStore** text box. Click **Next**.



3. Click on the **browse** button next to the **Path of the MediaStore** box to enter the appropriate path to your MediaStore.

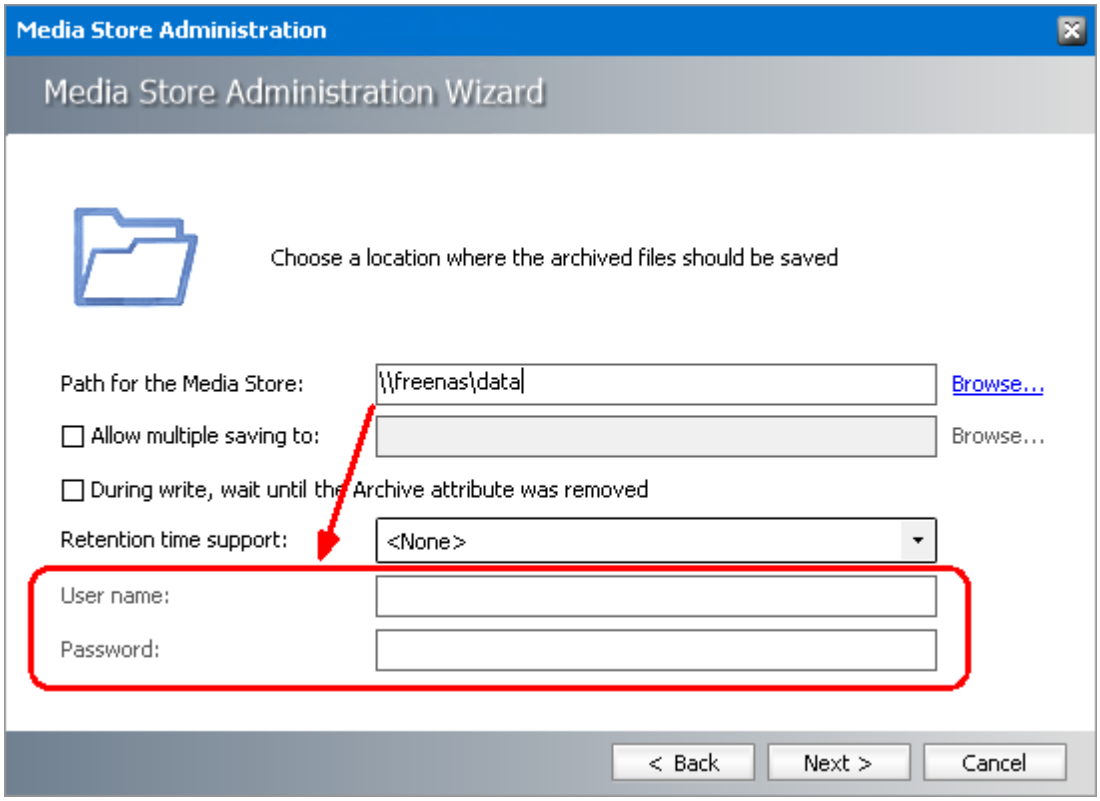
   NOTE: To create a new folder, use the **Make New Folder** button. Enter the name for this new folder, e.g. *Store* and click **OK**.



If your MediaStore is a network share, you can specify which **User** (with its **Password**) should access the share. You have to specify the user if:

- your share is not accessible by the user which runs the HSM services;
- you need a different user for each store;
- you want to create more “Simple Stores” accessing network shares; In that situation consider the user’s access permission to the store paths

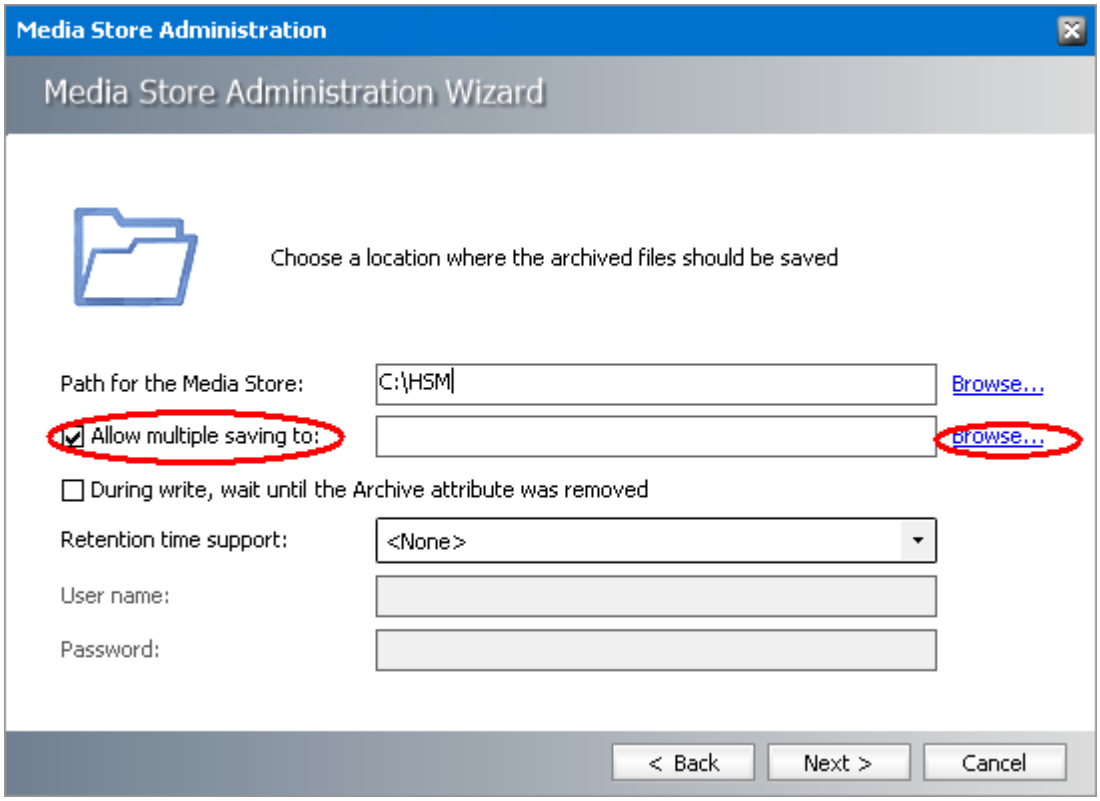
NOTE: The specified user does not need to be a known local user.



4. Should you wish to archive files simultaneously to some other location as well, select the **Activate multiple saving** check box. Use the **browse** button, similarly as above, to specify a second path.

   The files will be archived to this second location, too.

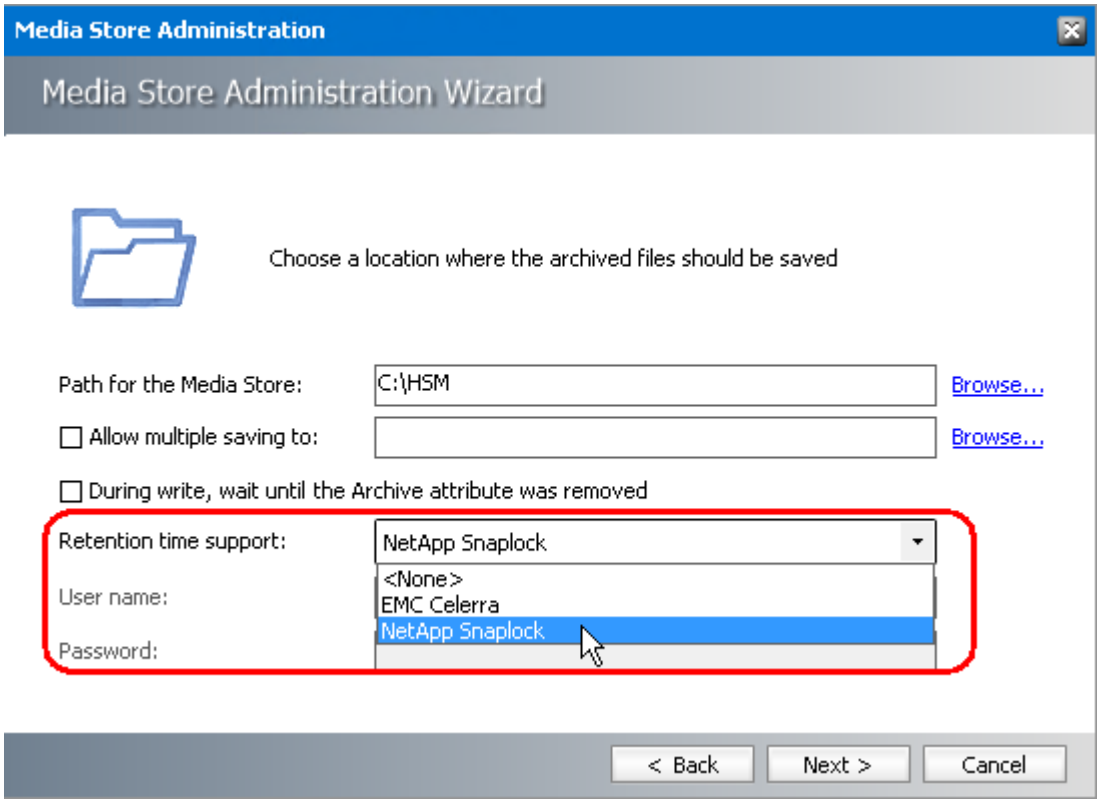
   NOTE: The second path can be anything that is reachable by a drive-letter or a network share, something accessible with Windows Explorer.



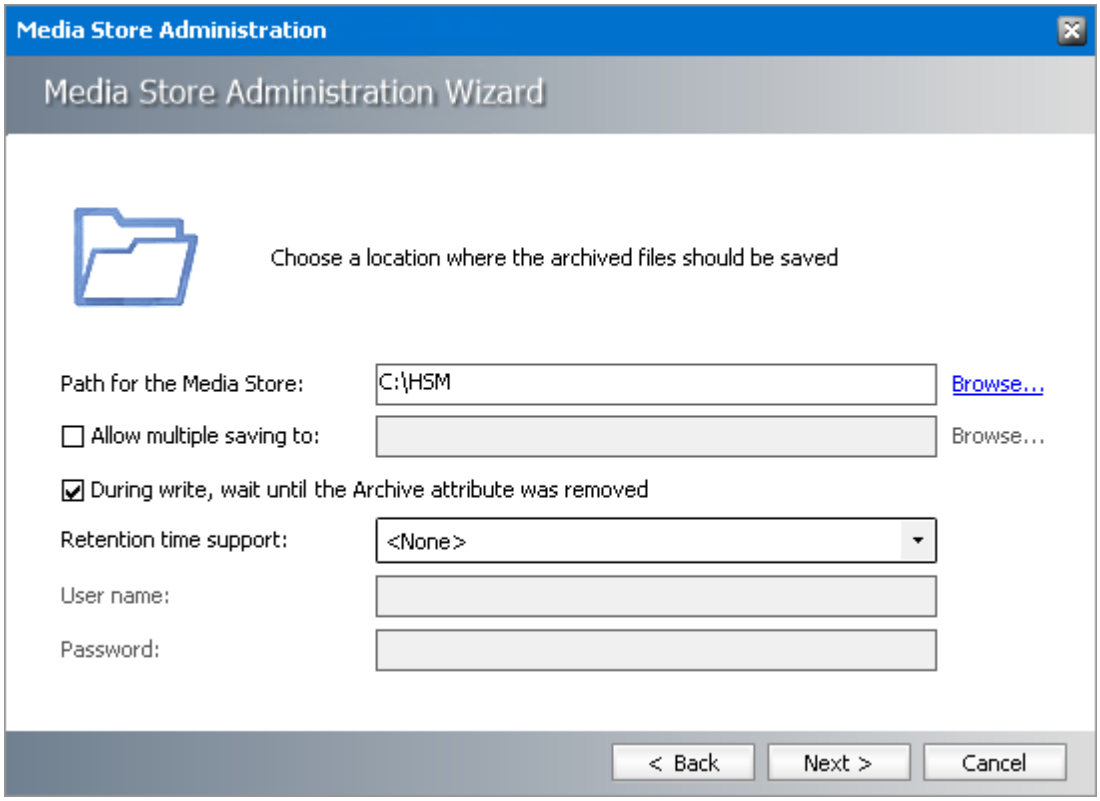
5. In the **Retention time support** drop-down box select the **NetApp SnapLock** option if you are using NetApp and want to use SnapLock to secure the compliancy with law regulations regarding archiving of electronic documents. (e.g. HIPAA, OFRS, COSO etc.)

   In case you are using EMC Celerra and you wish to use its retention times for your archived files, select **EMC Celerra**.

   NOTE: In case you are using *multiple saving* and *retention time* support both must be stores supporting the same retention type.



6. If you are storing to SAM-FS (a kind of NAS - Network Attached Storage) check the **During write, wait until the "archive" attribute was removed** check box. With this feature activated you have configured the SAM-FS to remove the "archive" attribute after the file was copied into a safe location (e.g. after it was copied to a tape drive). If you have finished, click **Next**.

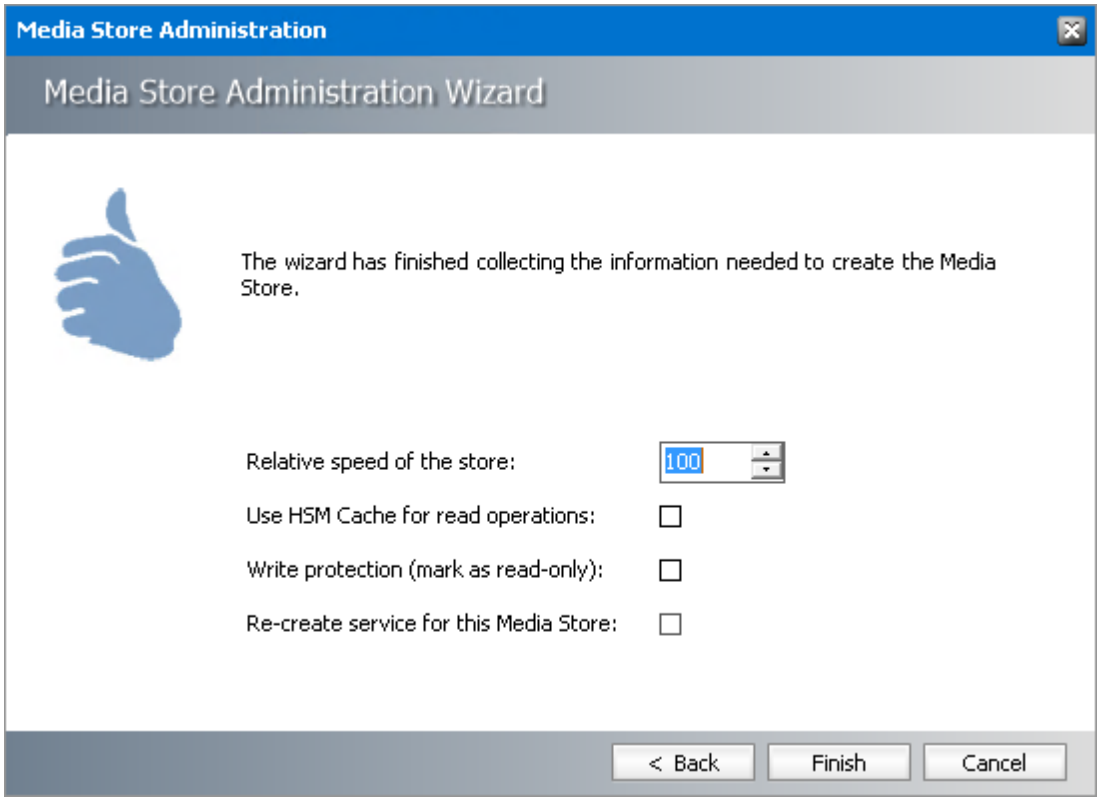


7. In the following dialog the **Relative speed of Store** text box represents the relative speed of this store compared to other stores.

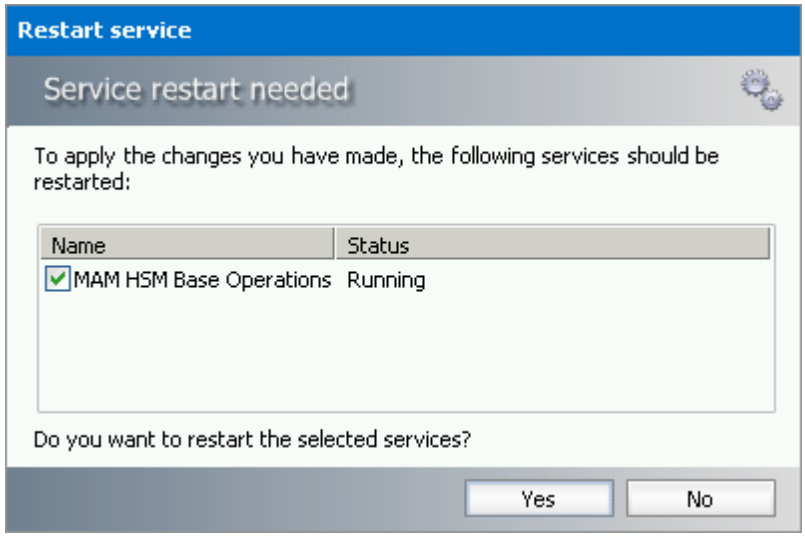
   If HSM should copy files into the cache when reading from this store, check **Use HSM Cache for read operation**.

   If this media should be read-only, check **Write Protection** check box (only supported for “Jukebox, Harddisk, Network” and “Simple Path”).

   Click **Finish**.



8. You will be asked to restart the service to apply the changes. To restart, click **Yes**.



NOTE: Should you be using several MediaStores, you need to repeat all steps as described in this section for each of them.

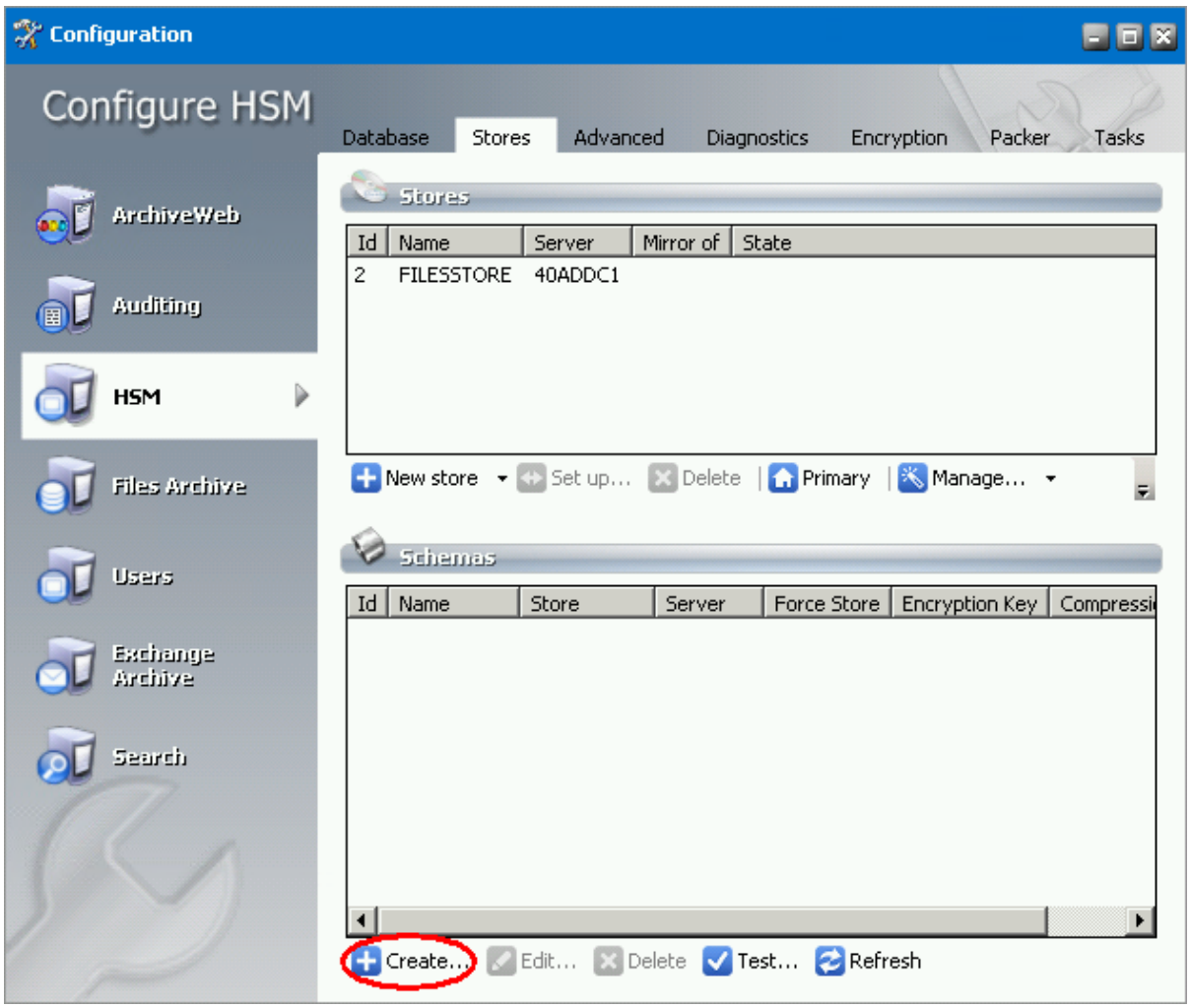
Specifying a Schema

Having a store ready is not enough. We need a schema, which is basically the path to the MediaStore. This schema needs to be registered in the HSM database.

Therefore, in this phase we will specify a schema and will assign the MediaStore having been created in the previous section to this schema. As mentioned previously, you may create as many schemas as you wish. For each schema you need to choose a store where the files will be archived.

To specify a schema, do as follows:

1. In the **Configuration** tool, on the **Stores** tab click the **Create** button.



NOTE: When there are already some schemas created, buttons under the Schemas list view can be used to administer them:

Edit – change the selected schema settings
Delete – delete the selected schema
Test – test the selected schema functionality
Refresh – refresh the list view

2. In the **HSM Schema** window enter the following information:

In the **Store** drop-down list select the appropriate store.

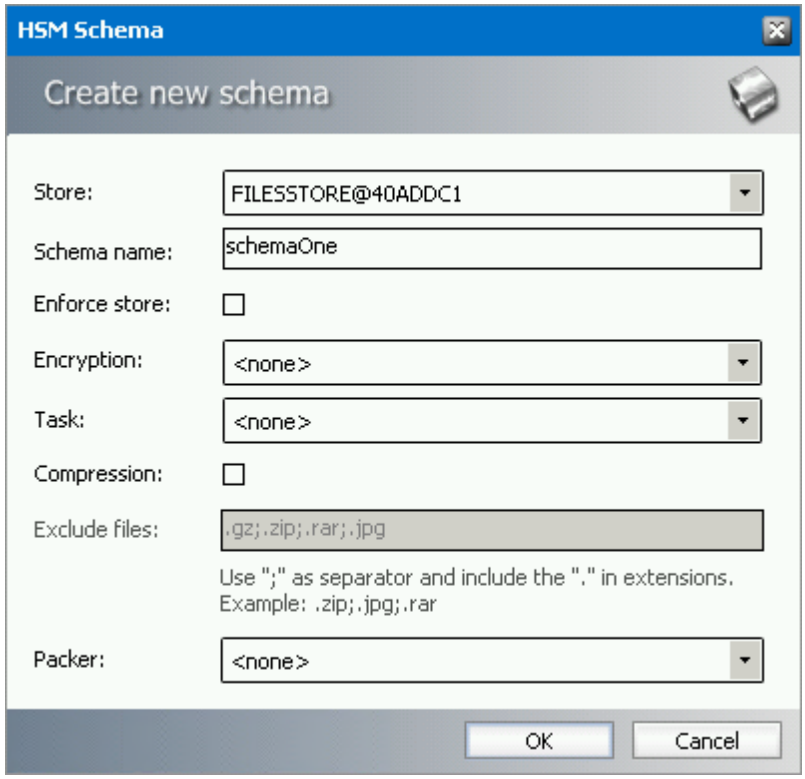
In the **Schema name** text box enter a name for your schema, e.g. *schemaOne*.

When selecting the **Enforce Store** check box, you enable duplicate archiving. For example: you archive a file in scheme 1 (using Store A) and them archive it again in scheme 2 (using store B). The file is recognized as duplicate but is written to both stores.

In the **Encryption** drop-down list select the appropriate encryption.

In the **Task** drop-down list select the task you want to assign to the schema. The task will run during the archiving of a file, e.g. copying the file to another media store. (Tasks are created on the **Tasks** tab.)

NOTE: Tasks with delete operation are not listed in drop-down list.



If you select the **Compression** option then compression will be applied at archiving.

It is possible to set exceptions for the files you do not want to compress. List the desired extensions in the **Exclude files** text box. Please use semicolon ";" to separate individual extensions and include dot "." in the extension.

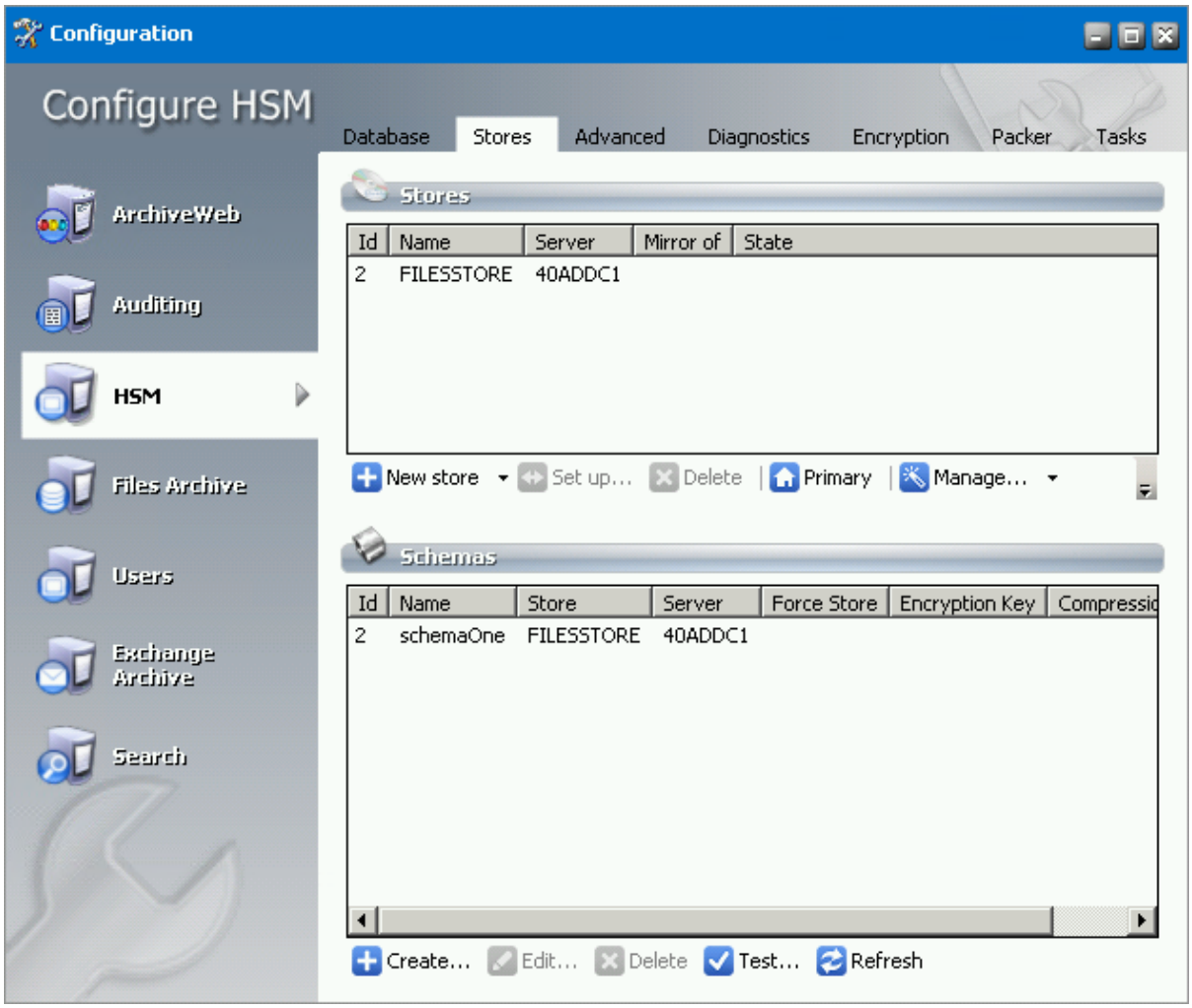
In the **Packer** dropdown box you can select a packer if any is created on the **Packer** tab. Packers are joining multiple files stored in HSM into large ZIP archives. It is better to have several large files than a plenty of small ones – the disk space utilization is more efficient in this case, because it helps to avoid internal disk fragmentation.

NOTE: It's not possible to have packer and task selected at once. If you need to use packer together with some other task operations, a packer operation can be defined directly as a task operation.

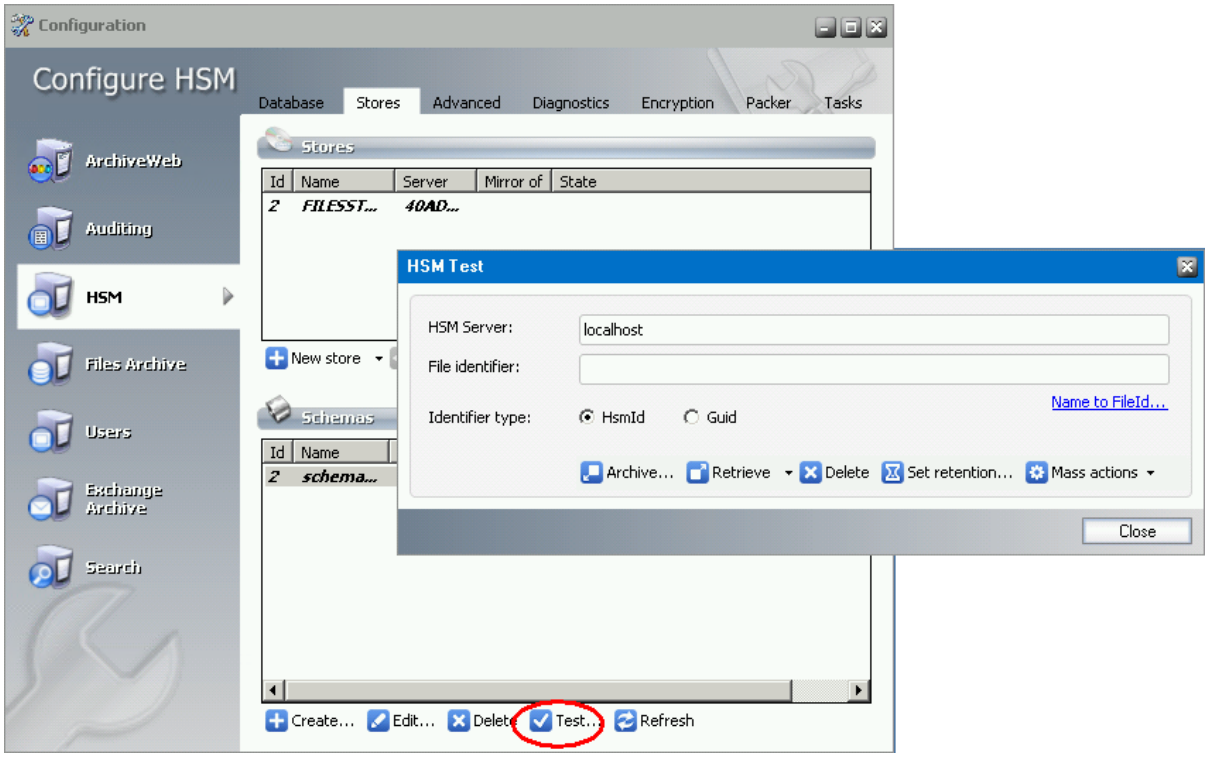
Click **OK**.

3. After clicking **OK** you will be asked to restart the *HSM Base Operation* service. Click **OK**. Then the schema appears in the Schemas list view.

   Do not click **Close** yet. It is good to check at this point whether archiving functions.



4. To check if archiving functions, click the **Test** button. The **HSM Test** dialog pops-up where archive, retrieve and delete operations should be tested.



5. Click **Archive**. In the pop-up Archive dialog select the **Target schema** you want to test. No further configuration is necessary. However, it is possible to set **Retention time** for the test file:

    - Fixed value
    - Infinite
    - Indefinite (i.e. the retention time is not set specifically but can be defined later)

    You can also choose to use **generated test files** or **use a specific test file** (user generated, e.g. for testing big file archiving) or choose other testing options:

    Make each file unique – new unique string is generated after each test archiving

    Use invalid checksum – test checksum verification

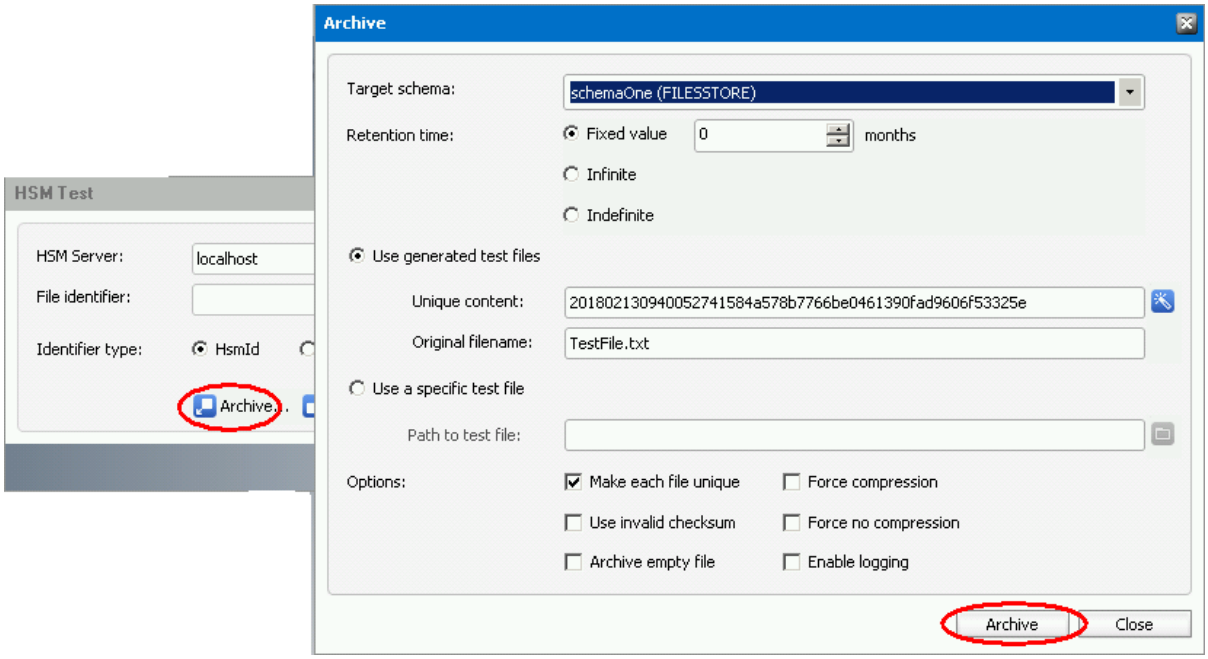
    Archive empty file – check to test empty file archiving

    Force compression – check to compress test files

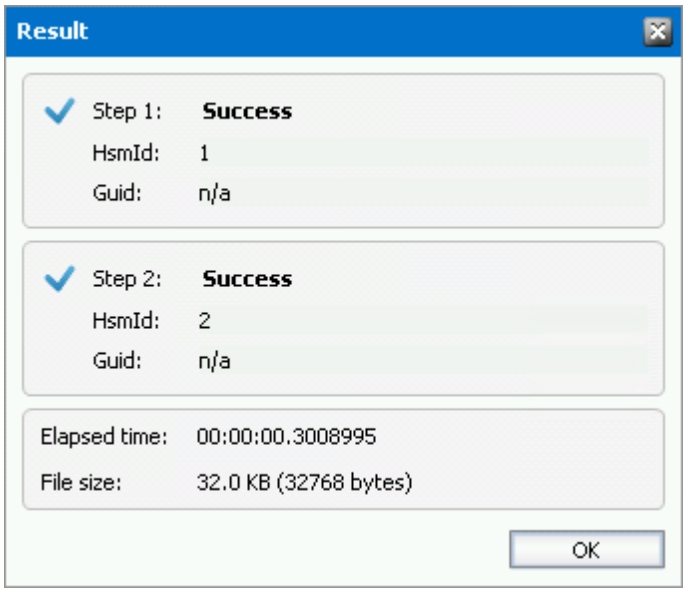
    Force no compression – check for no compression even if the compression is enabled

    Enable logging – check to log test operation

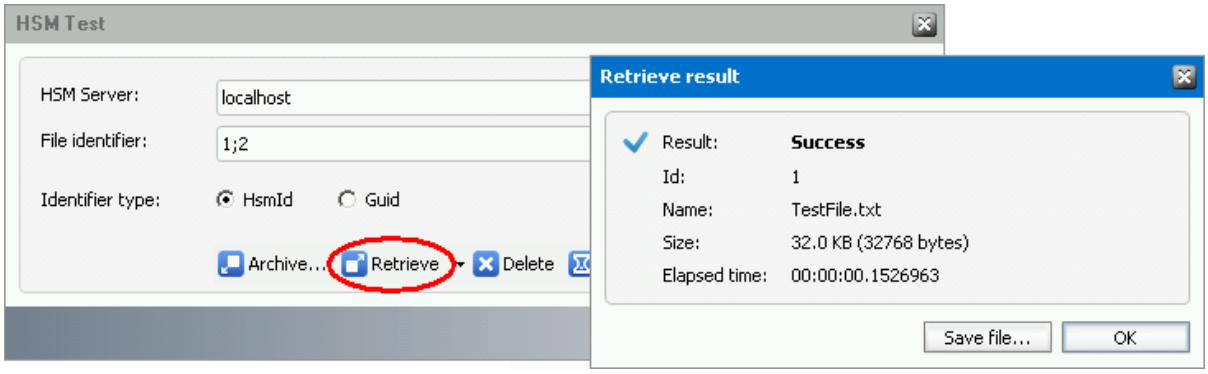
    Then click **Archive** to check whether archiving functions properly.



6. After successful archiving click **OK**, then **Close**.



7. Click on the **Retrieve** button to check, whether retrieving functions properly. Click **OK** to close the **Result** window for each file identifier.



8. If everything works, close the Test window. Close also the **Configuration** tool.

Once the HSM is installed and configured as described above, you may proceed with manual installation of Archive Manager.

Besides the settings above which are necessary for correct deployment of HSM, several additional configuration options are available in **Configuration** tool. Additional configuration is optional but it can enhance HSM performance and provide administrator with diagnostic, encryption, pack and async task possibilities. Detailed instructions on how to manage additional options can be found in the next section "*Optional Configuration*".

3

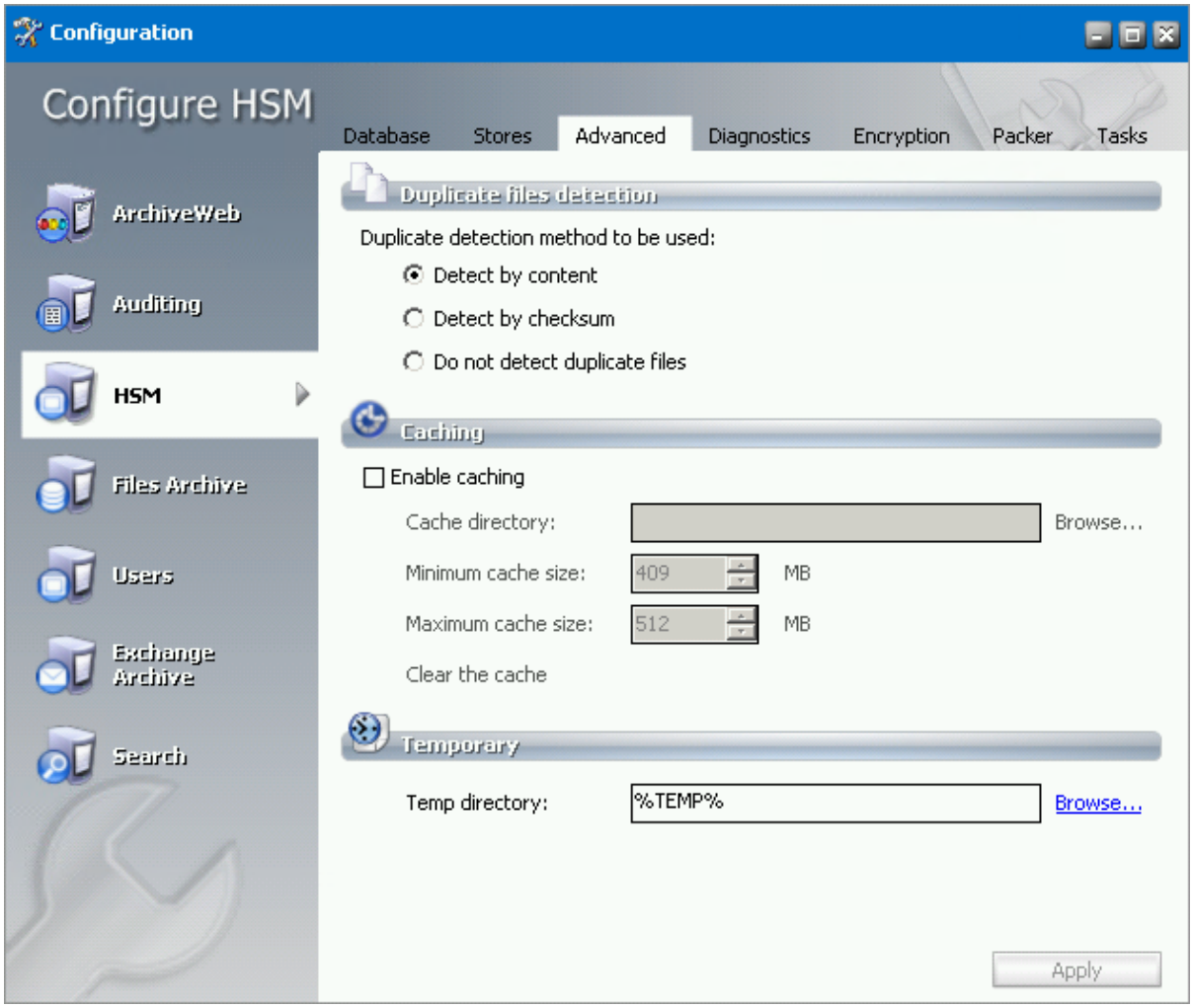
Optional Configuration

Additional configuration options of HSM in Configuration tool described in this chapter are optional. However, they provide administrator with diagnostic, encryption, pack and async task possibilities on the following tabs:

- Advanced
- Diagnostics
- Encryption
- Packer
- Tasks

Advanced tab

This tab is used to configure the more advanced settings of HSM as single instancing, cache settings and temporary folder. After configuring all options press the **Apply** button.



Duplicate files detection

Since the HSM system includes the Duplicate Files Detection service, it means that identical files are stored only once. In the **Duplicate files detection** section you may specify the detection method:

a) Select the **Detect by content** option, should you wish to use the size, checksum and content for detection.

b) Select the **Detect by checksum** option, should you wish to use the size and checksum for detection;

c) Select **Do not detect duplicate files** option, should you wish to disable this detection

WARNING: In case the *Force in store* is enabled, the file is stored in both stores.

Caching

Use caching in case of slow storages (tape etc.). HSM will cache the recently used files to speed up the retrieving process.

If **Enable caching** is checked, HSM will copy all retrieved files to an HSM internal cache. To set the **Cache directory** (which should be a local hard disk), use the **Browse** button next to the respective text box. If you have a cluster, the HSM will know that each installation has its own path.

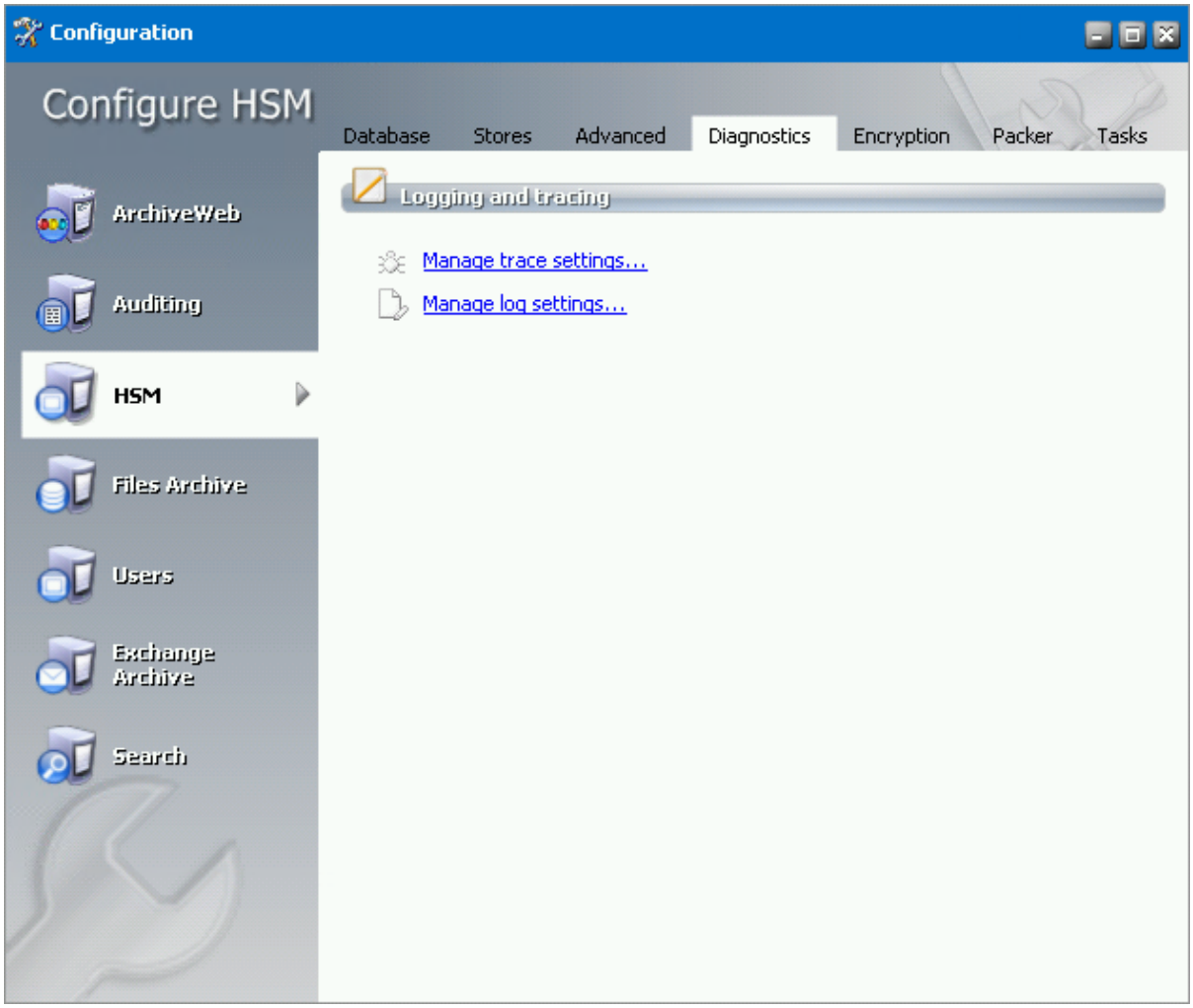
Set the **Minimum cache size** and **Maximum cache size** as well. The **Minimum size** should be about 80% of the cache size. If the cache is full, HSM will delete files (the oldest first) until the cache reaches the “minimum size”.

NOTE: To choose which Media Store should be cached, use the MediaStoreAdministrator tool. It is started when you click Launch on the Stores & Schemas tab.

The HSM stores temporary files created during duplication detection, compression etc. in temporary directory. Its location can be set in **Temp directory** text box. Usage of environment variables is allowed in this box (e.g. %TEMP% denotes the temp folder of the currently logged on user).

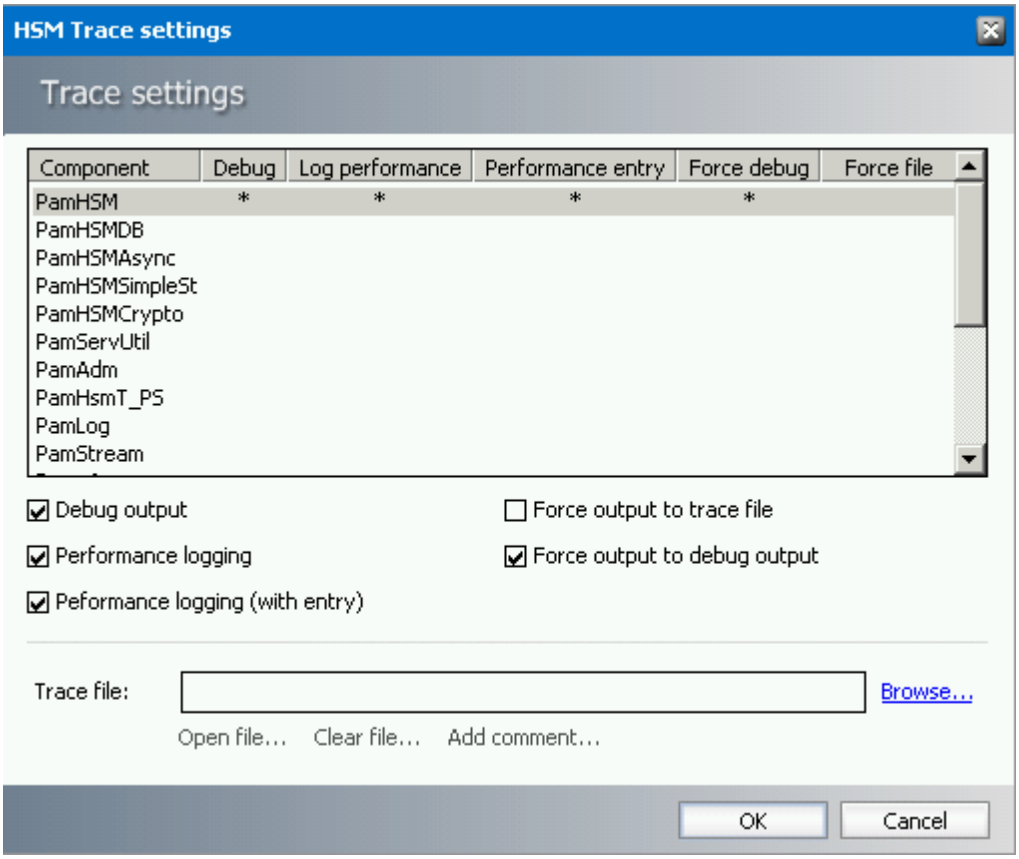
Diagnostics tab

From time to time administrators need to check systems they manage, examine and analyze their behavior. This tab provides access to features that facilitate this task. Logs and tracing record HSM actions specified by the administrator at the defined extent.



Manage trace settings

In the HSM Trace Settings configuration you can enable various kinds of loggings for the specific HSM components. Select the component in the list and then configure it by checking/unchecking the desired check boxes. Multi-select is possible.



You can enable verbose logging (**Debug Output**), two kinds of performance loggings (logging information after a specific operation is completed or before a specific operation begins – **Performance logging** and **Performance logging (with entry**) and choose whether you want to re-direct outputs either to debug output (**Force output to debug output)** or to the given trace file (**Force output to trace file**). In the case of **Force output to trace file** the path has to be specified in the **Trace File box**. The trace information will be logged there. You can also Open the trace file with the **Open file** button or delete its contents with the **Clear File** button. If you clear the file then the file itself won't be deleted. Use **Add comment** in case you wish to add some text to the file.

After changing the settings you want click the **OK** button. If you want to discard them click the **Cancel** button.

Manage log settings

In the Log settings dialog configure the overall HSM logs to your needs:

Include message levels – define which information should be logged

- **Errors only**
- **Errors and warnings**
- **Errors, warnings and Information**

NOTE: "Error" and "Warning" is internal classification of log entries.

Debug output – check to enable verbose logging

Log file – check to save the messages in log files

Path – set logs location

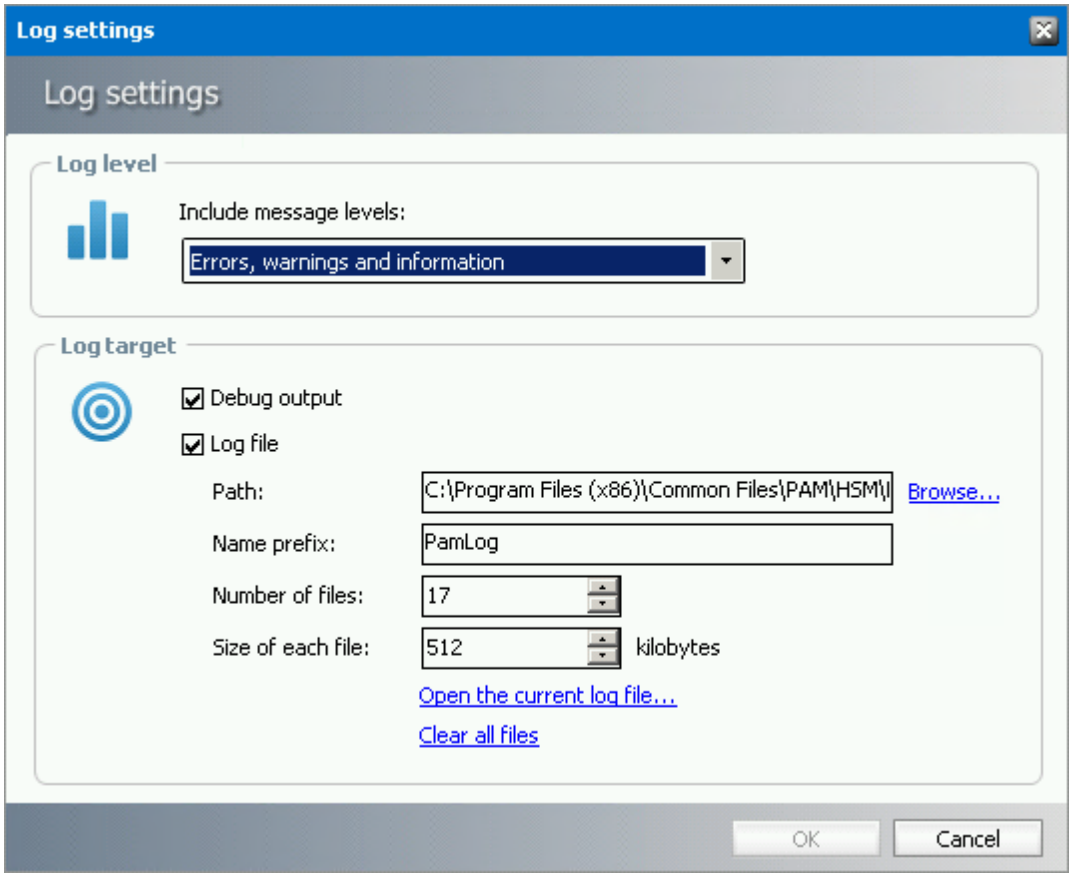
Name prefix – define naming convention; log file name will include this prefix and a number

Number of files – if a new log file should be created when the limit is reached, the oldest log file will be deleted

Size of each file – when the defined size is reached, new log file will be started

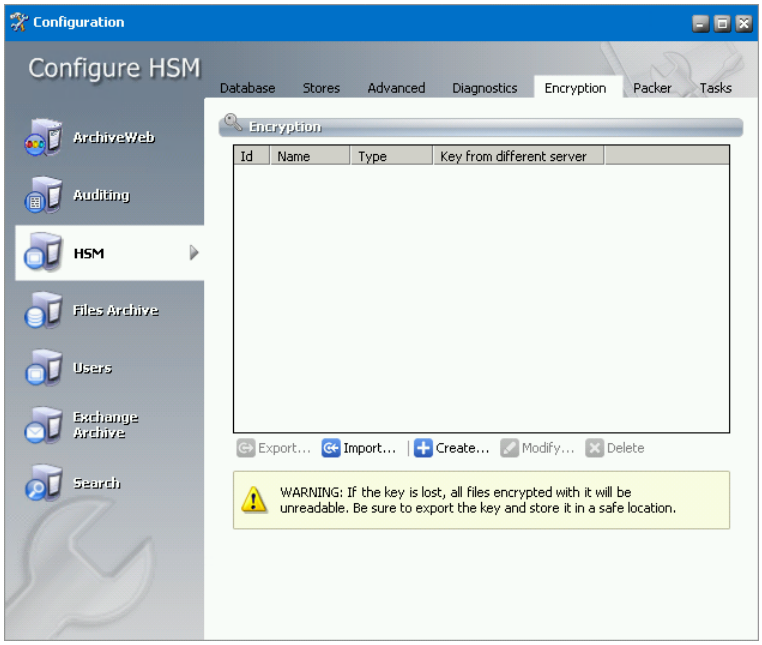
Click **Open the current log file** to open it.

Clicking the **Clear all files** will delete all logs.



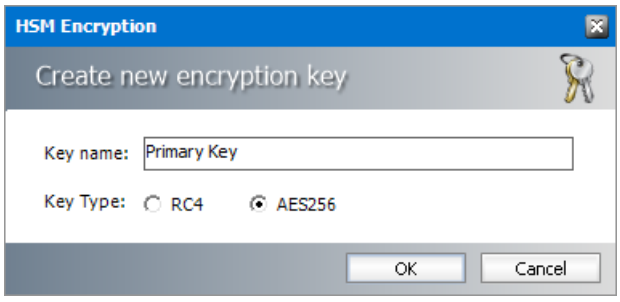
Encryption tab

The Encryption tab allows you to manage encryption keys that are used to safeguard your archived items stored in HSM.



Steps to create an encryption key

1. In the *Encryption* tab, click **Create**. The *Create new encryption key* window opens.

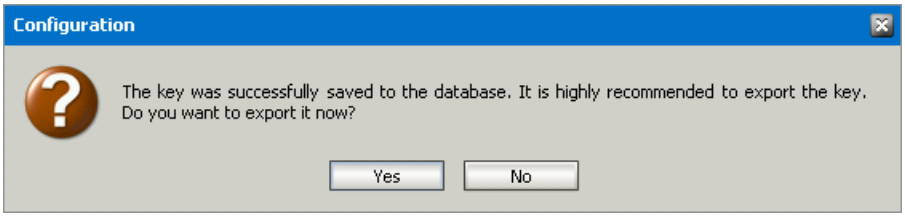


   Enter the information as described below:

   Key name - display name of the encryption key.

   Key type - Select one of the industry standard encryption ciphers **RC4** or **AES256**. Between the two, AES256 is a relatively new and very complex 256-bit block cipher, and RC4 is a very old and simple stream cipher.

2. Click **OK** to create the encryption key. The *Configuration* window opens.

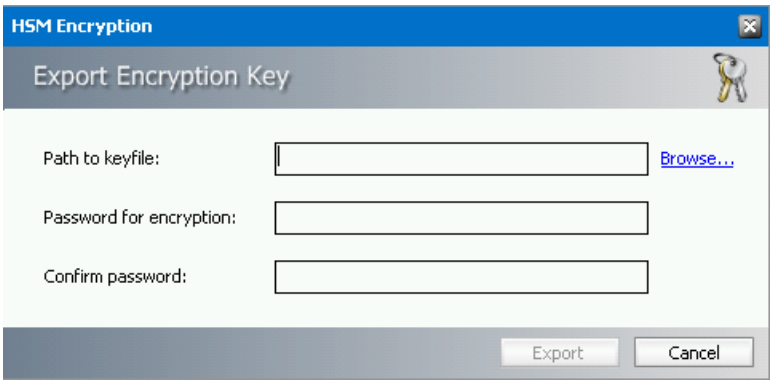


3. Click **Yes** to export the key or click **No** to export it later. If you click **Yes**, the *Export Encryption Key* window opens. See the section below for steps to export the encryption key.

> **IMPORTANT:** Always export and store encryption keys in a safe location. If the key is lost, it will not be possible to read the encrypted files.

Steps to export an encryption key

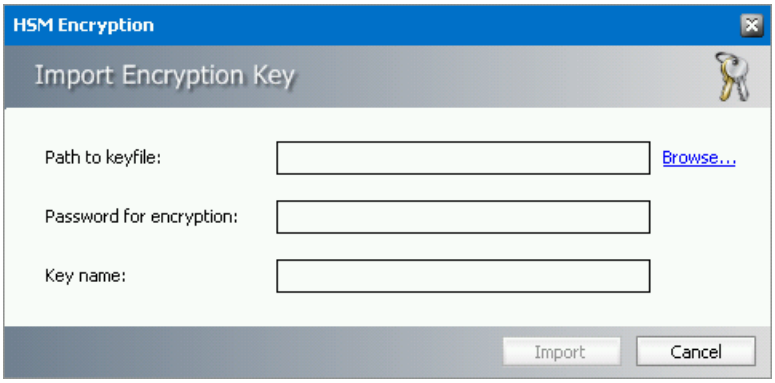
1. There are two ways to export an encryption key:
   a. Select an encryption key from the encryption key list and click **Export**.
   b. Create a new encryption key and click **Yes** in the *Configuration* window that opens after you have created the key.
2. In the Export Encryption Key window, enter the information as described below.



   a. **Path to key/file** - location where the key will be exported. Click **Browse** to open the *Save As* window. The default location is `C:\Program Files (x86)\Common Files\PAM\HSM\Keys`. Keep the default or choose a location. Then enter a name for the encryption key file and click **Save**.
   b. **Password for encryption** - enter a password for the encryption file.
   c. **Confirm password** - enter the password again to confirm the password entry.
3. Click **Export** to export the encryption key.

Steps to import an encryption key

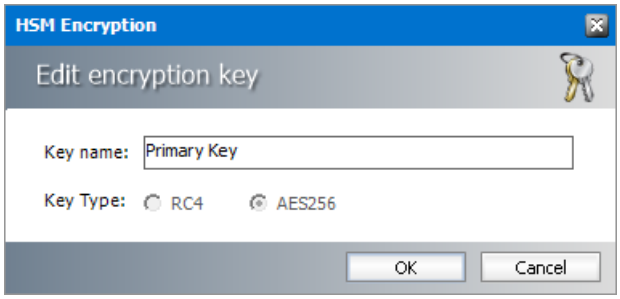
1. In the *Encryption* tab, click **Import**. The *Import Encryption Key* window opens.



2. Enter the information as described below:
   a. **Path to key/file** - location from where the key will be imported. Click **Browse** to select a location.
   b. **Password for encryption** - enter a password for the encryption file.
   c. **Key name** - name of the encryption key file.
3. Click **Import** to add the encryption key to the HSM encryption key list.

Steps to modify an encryption key

1. Select an encryption key from the encryption key list and click **Modify**. The Edit Encryption Key window opens.



2. You can change the *Key name* of the encryption key but you cannot change the *Key Type*.
3. Click **OK** to save the change.

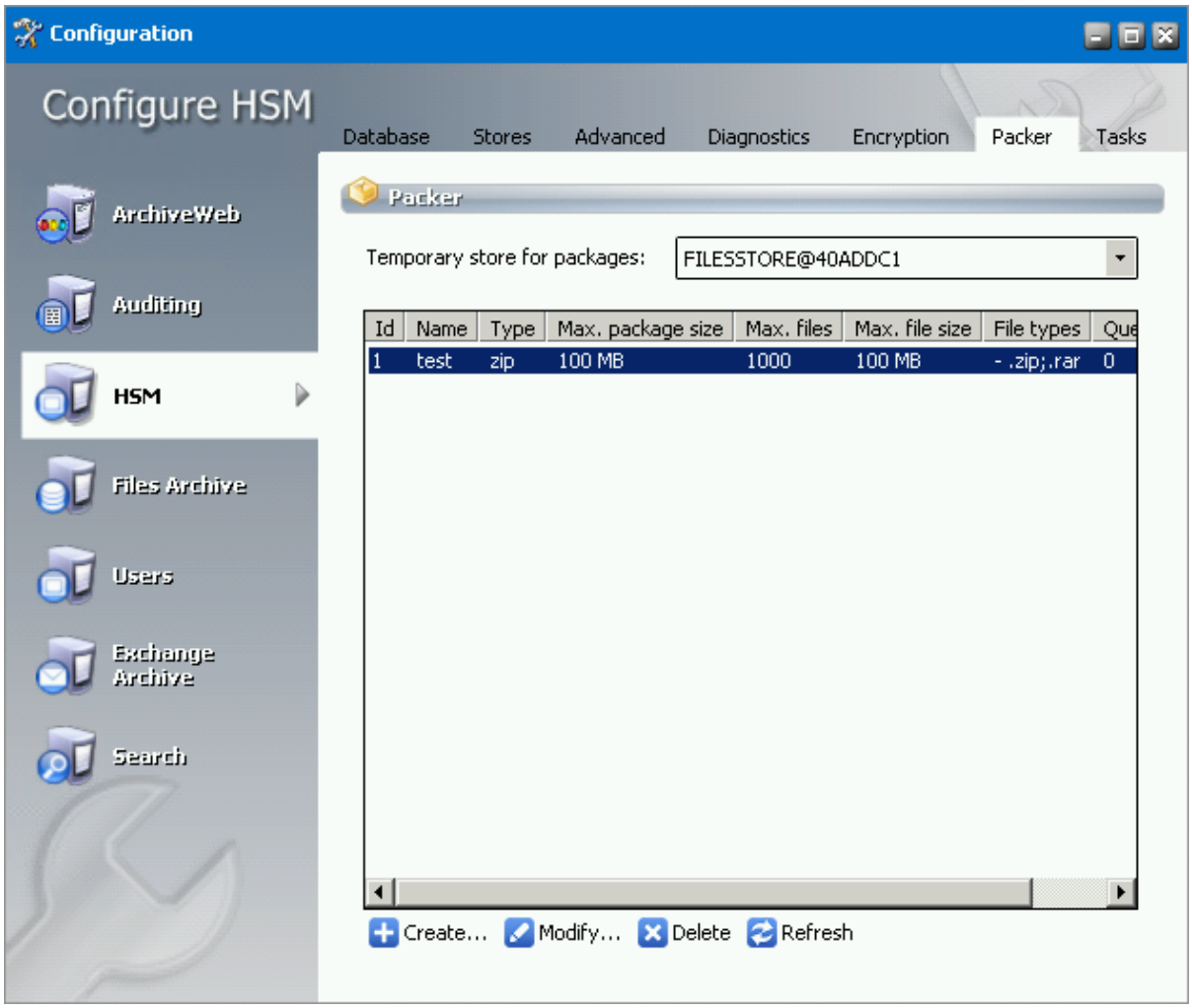
Steps to delete an encryption key

1. Select an encryption key from the encryption key list
2. Click **Delete**. *A confirmation* window opens.
3. Click **Yes** to confirm the deletion of the encryption key.

Packer tab

Packers are joining multiple files stored in HSM into large ZIP archives. It is better to have several large files than a plenty of small ones – the disk space utilization is more efficient in this case, because it helps to avoid internal disk fragmentation.

Packers can be created and managed on the **Packer** tab. Created packers can then be assigned to specific schema on the **Stores** tab.



First select the store in **Temporary store for packages** dropdown. It will be the temporary store for archived files before they got packed. Then the packed files will be moved to the final store (it can be the same store as well).

To create a packer, click **Create**. The HSM Packer dialog pops-up. Configure the settings:

Name – enter packer name

Type – the file to be used by the packer

Max. package size – if the specified limit is reached, new package will be created

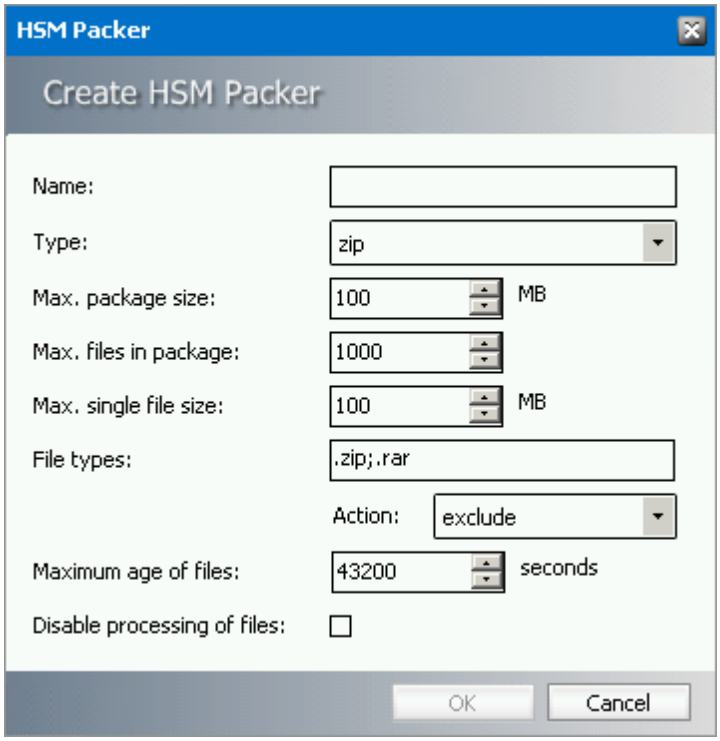
Max. files in package – package starts to be created when the specified number of files is reached

Max single file size – if the file size is bigger than the specified value, the file will not be included in the package (otherwise it would be much time consuming)

File types & Action – allow specifying file types to be included / excluded in/from the package

Max age of files – is files to be packed are waiting in the packer queue longer than the specified value, a new package will be created

Disable – disable processing of files in the packer queue



Following table displays how archived files in HSM are handled during 'Asynchronous packer' task process:

Temporary store for packages	Source Store result	Target store result
Same as Source store (*)	Original archived files are deleted after they are compressed and stored in Temporary store for packages.	ZIP container with archived files
Different as Source store (*)	Original archived file remains at store after they are compressed	ZIP container with archived files

	and stored in Temporary store for packages.	

Temporary store for packages: HSM store that is used by packer process to store compressed temporary files that are subsequently stored in ZIP container. Current version of HSM uses only GZ compression.

Source store: HSM store that is processed by 'Asynchronous packer' task.

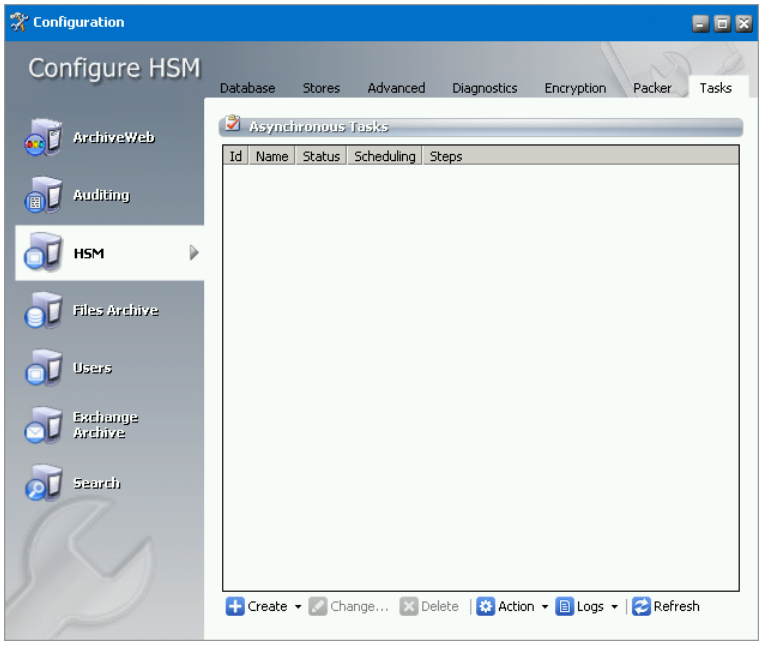
Target store: HSM store where ZIP containers are stored as a result of 'Asynchronous packer' task

NOTE: Files archived into HSM with compress option enabled at schema always remains at source store regardless settings of temporary store for packages. These files also do not use 'Temporary store for packages' since they are already compressed. This behavior is by HSM design.

Tasks tab

On this tab you can create asynchronous tasks for HSM. An *asynchronous* task can be performed at a later time and not immediately after its creation. Basic tasks are the following:

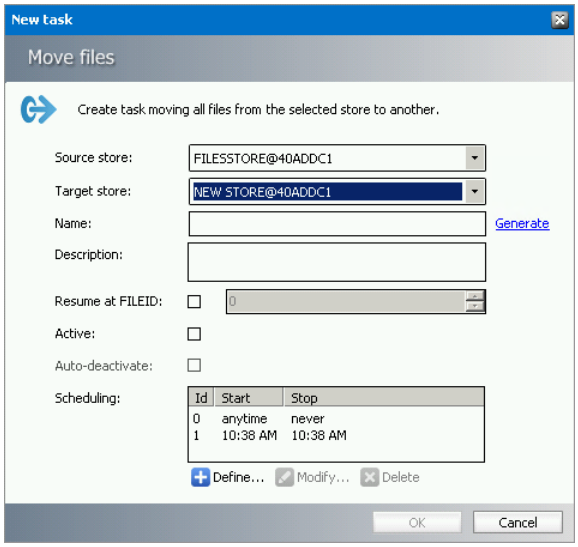
- **Copy** - copies archived items from a source store to a destination store.
- **Move** - moves archived items from a source store to a destination store.
- **Encrypt** - encrypts files in the specified store with a selected encryption key.
- **Advanced** - define multiple tasks or sequence tasks based on specific criteria.



Creating Move / Copy task

NOTE: Before creating any asynchronous task, stores must be created under the **Stores** tab.

1. Click **Create** > **Move task** (or **Copy task**). The *Move files* (or *Copy files*) window opens.



Enter the configuration details as described below:

a. **Source store** dropdown menu select the store from which the files will be moved (copied).

b. **Target store** dropdown menu select the store to which the files will be moved (copied).

c. **Name** text box type the task display name or click *Generate* to fill in the text box with generic name.

d. **Description** - add a description about the task.

e. **Resume at FILEID** - select the check box if you want the task to "remember" the last processed file and resume at the next one when it starts again after a pause. (The textbox displays the file ID of the latest processed file.)

f. **Activate** - select the check box to enable the task.

g. **Auto-deactivate** - select the check box to deactivate the task when it completes. The check box is available only when **Resume at FILEID** is checked.

h. **Scheduling** - Sets the task run time. Besides the default perpetual unlimited scheduling, you can add your own start time and stop time by clicking **Define**. There can be several schedulers defined. Then select the actual scheduling time. The task will be started every day at the defined time.

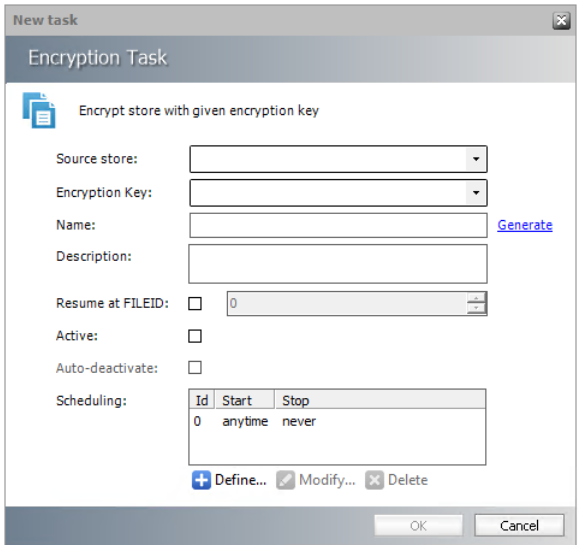
   NOTE: Task scheduling can be modified when you select the task from the list and click **Modify**. If *anytime* is selected the task starts whenever the MAM HSM Asynchronous Operations service starts.

2. Once the task is configured, click **OK**. The task displays in the *Tasks* list.

Creating Encryption Task

NOTE: Before creating any asynchronous task, stores must be created under the Stores tab.

1. Click **Create** > **Encrypt task**. In the *Encryption Task* window opens.



Enter the configuration details as described below:

a. **Source store** dropdown menu select the store to which the files will be encrypted

b. **Name** text box type the task display name or click Generate to fill in the text box with generic name.

c. **Description** - It is a good practice to add a short Description of the task.

d. **Resume at FILEID** - Select the check box if you want the task to *remember* the last processed file and resume at the next one when it starts again after a pause. (The text box displays the file ID of the latest processed file.)

e. **Activate** - Select the check box to enable the task.

f. **Auto-deactivate** - Select the check box if you wish to deactivate the task as soon as it completes. The check box is available only when **Resume at FILEID** is checked.

g. **Scheduling** - specify the task run time. Besides the default perpetual unlimited scheduling, you can add your own start time and stop time by clicking **Define**. There can be several schedulers defined. Then select the actual scheduling time. The task will be started every day at the defined time.

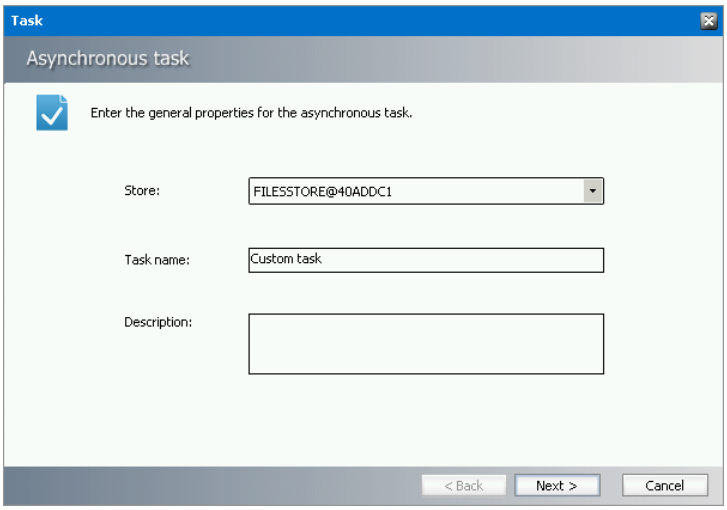
   NOTE: Task scheduling can be modified when you select the task from the list and click **Modify**. If *anytime* is selected the task starts whenever the MAM HSM Asynchronous Operations service starts.

2. Once the task is configured, click **OK**. The task displays in the *Tasks* list.

Creating Advanced Task

Advanced task allow configuration of specific task criteria. To create the Advanced task:

1. Click **Create** / **Advanced** option from the menu. Task wizard opens.



In the first dialog enter the general task configuration:

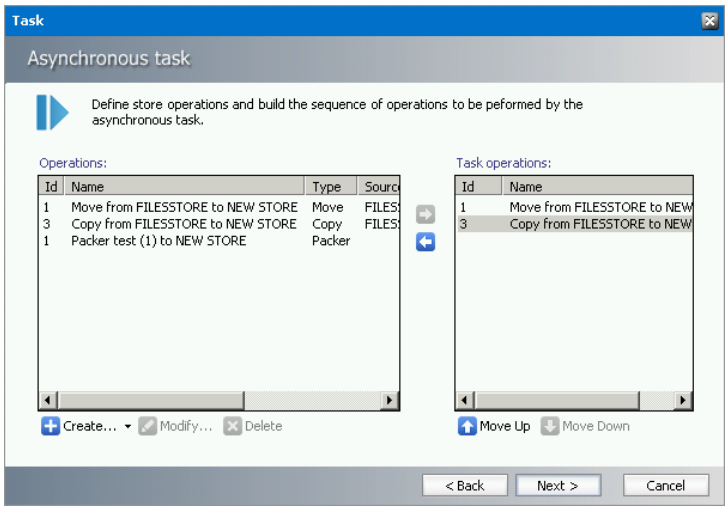
a. **Store** – select the source store for which the task should apply

b. **Task name** – enter tasks display name

c. **Description** – it's a good practice to add short task description

d. Click **Next**.

2. Advanced task can consist of several operations. This dialog allows you to define the operations and the sequence in which they should be performed. To do so, select the operation in the **Operations** list and click the arrow to add the operation to the **Task operations** list. The operation sequence can be customized easily by selecting the desired operation and moving it up or down by clicking the **Move up** / **Move down** arrows under the list.

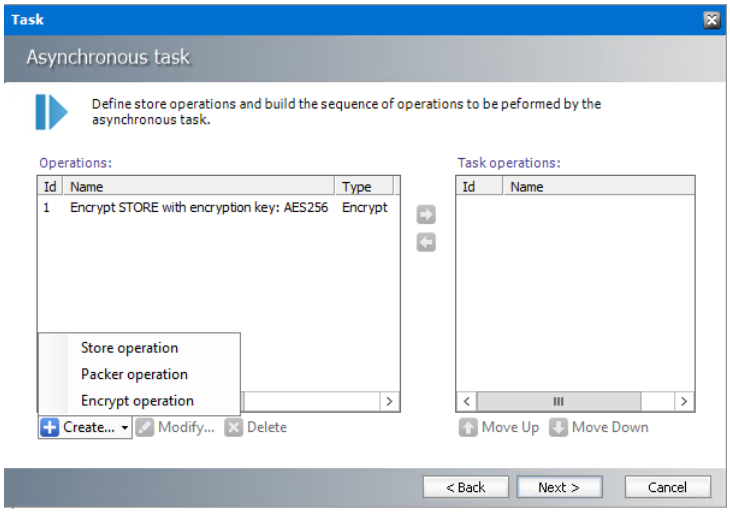


3. In case no operation is created in the **Operations** list or you wish to create a new one, click the **Create** button. You will be able to create:

   a. Store operation (Copy, Move and Delete) or

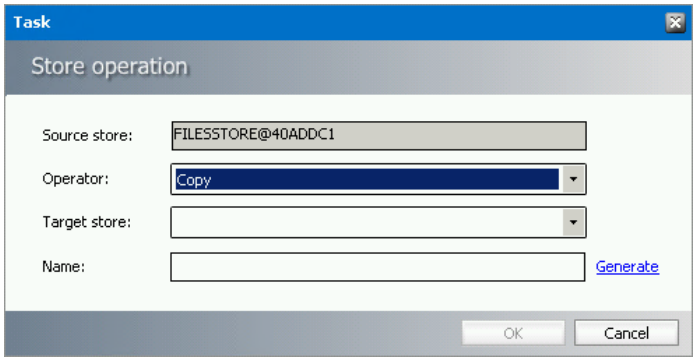
   b. Packer operation

   c. Encrypt operation



Store operation

a. In case the **Create**/**Store operation** has been selected, the Store operation configuration dialog opens. The source store will be the store you have selected in the previous dialog. In the dialog enter the operation configuration:



   i. **Operator** – select the type of store operation you wish to create (Copy, Delete, Move)

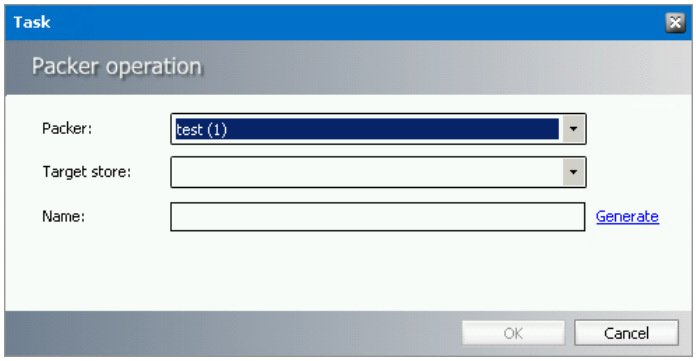
   ii. **Target store** – target store where ZIP archives are stored

   iii. **Name** – Name of the operation. To generate the name automatically click **Generate** button.

b. To confirm, click **OK**.

Packer operation

a. In case the **Create**/**Packer operation** has been selected, the Packer operation configuration dialog opens. In the dialog enter the operation configuration:



i. **Packer** – select the packer which the task should apply. Packers are defined in **Packer** tab.

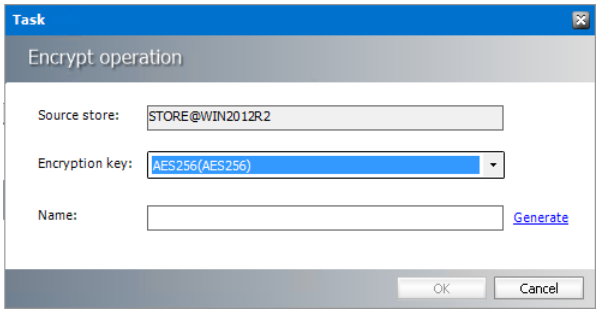
ii. **Target store** – target store where ZIP archives are stored.

iii. **Name** – Name of the operation. To generate the name automatically click **Generate** button.

b. To confirm, click **OK**.

Encrypt operation

a. In case the Create/Encrypt operation has been selected, the Encrypt operation configuration dialog opens.



i. **Source store** - will be the store you have selected in the previous dialog.

ii. **Encryption key** – select the encrypt which the task should apply. Encryption key is defined in Encryption tab.

iii. **Name** – Name of the operation. To generate the name automatically click **Generate** button.

d. To confirm, click **OK**.

4. Click **Next**. Set up filters defining files to be processed from the source store. To do so, click the filter you want to use from the left pane:

a. Resume at – the task will start from the specified file

b. Schema – specifies the schema under which the files are store

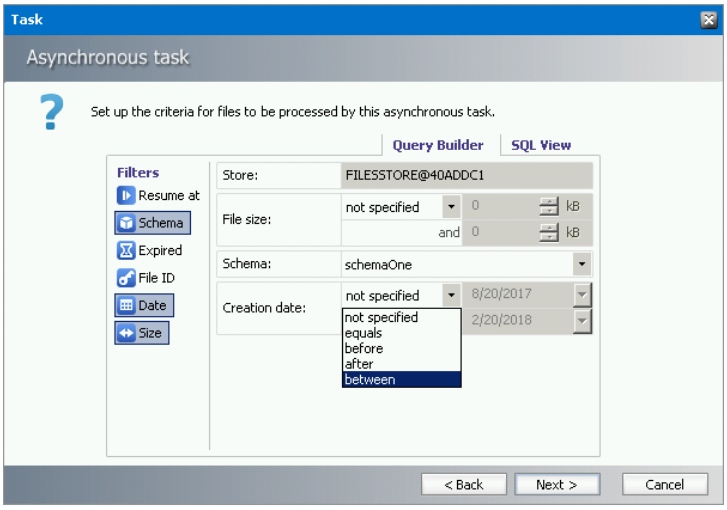
c. Expired – (yes/no) – specifies whether files where retention time has expired should be processed

d. File ID – specifies the ID of files

e. Date – specifies the archive date

f. Size – specifies the file size

5. The filter displays in the main pane where you can configure it. To remove the selected filter, click its name again.



SQl View tab – displays the defined filter criteria in SQL View. When you are modifying already existing task it is not possible to edit the query using the Query Builder directly. You have to edit your query in the SQL view. Should you want to use the Query Builder, you have to create a completely new query.

6. Click **Next**. Set the task scheduling. Make sure to check the **Active** check box to enable the task.

   a. To set **Run interval** when the task will be performed, select the desired option from the list or click **Define** button to set up custom interval.

   b. Check **Auto-deactivate** should you wish the task to become inactive as soon as it carries its work out. The check box is available only when **Resume at FILEID** filter is defined.

7. Click **Finish**.

Once the task is created, it displays in the Asynchronous task list view. Menu under the Asynchronous Tasks list provides access to the following functions:

- **Create** – create a new asynchronous task; two most common tasks can be created directly:
  - **Move task**
  - **Copy task**
  - **Encrypt task**
- **Advanced** - specific tasks can be created via wizard that is launched.
- **Change** – change settings of the task selected in the list view (for detailed description see the section “Creating Advanced Task”)
- **Delete task** – delete the selected asynchronous task

- **Action** – access to immediate Start, Stop or Restart of the selected task
- **Logs** – view log of the selected task or clear the respective log or logs of all tasks
- **Refresh** – refresh the tasks list

4

Addendum

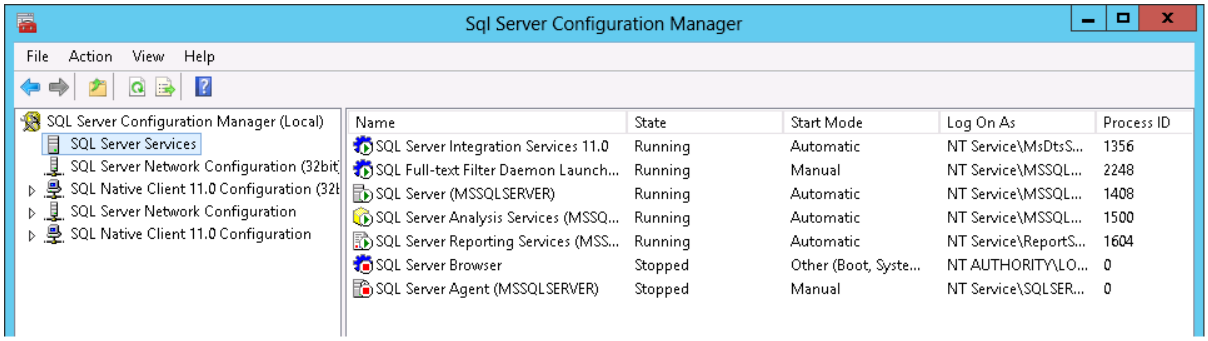
- Creating an MS SQL database with a database user 65
- Remote HSM Server 76
- HSM configured for Windows Server firewall 79

Setting up an MS SQL Server database

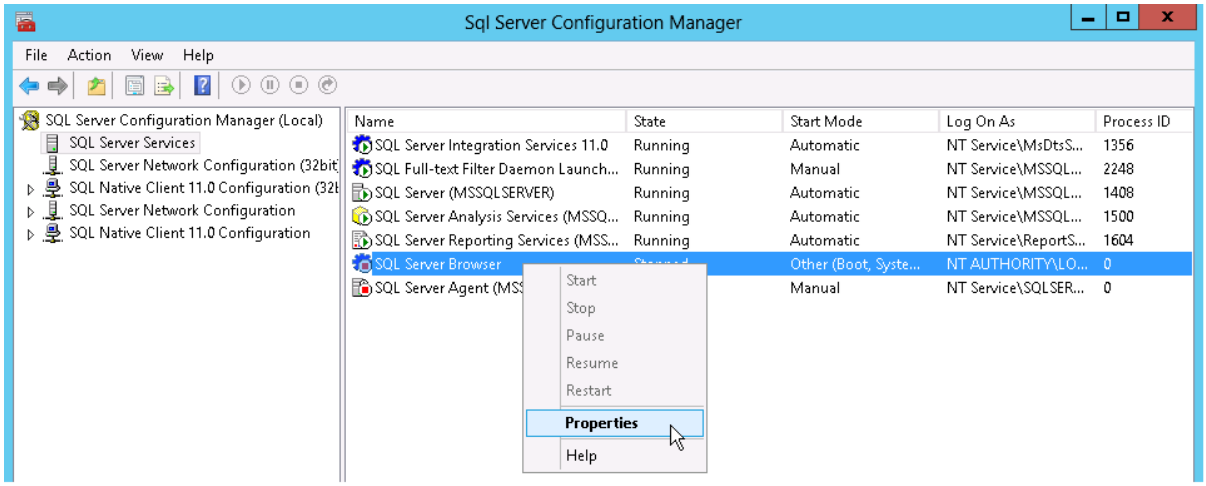
When planning to install HSM, an empty database and an appropriate database user must be created before running the setup. This section guides you through the configuration of a SQL Server 2012 database with a database user. In case of higher versions, you can use this as a reference.

To configure your SQL Server 2012:

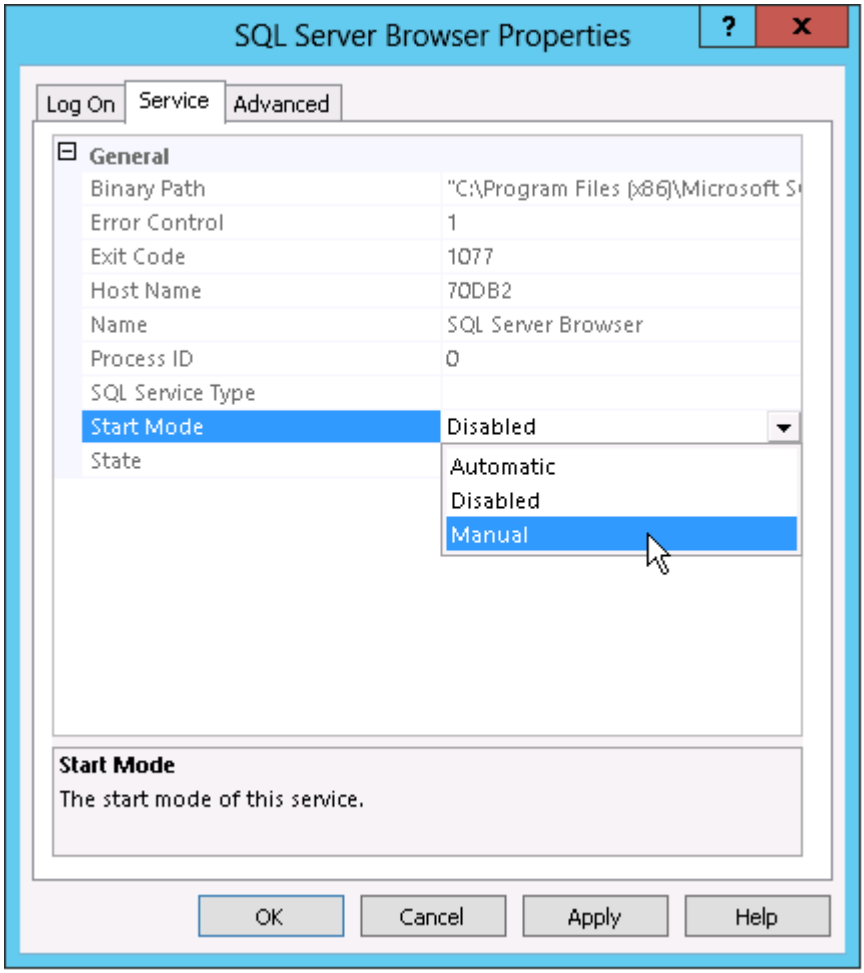
1. Open the **SQL Server Configuration Manager** and click the **SQL Server Services** node. Both the **SQL Server (SERVERNAME)** and the **SQL Server Browser** services have to run.



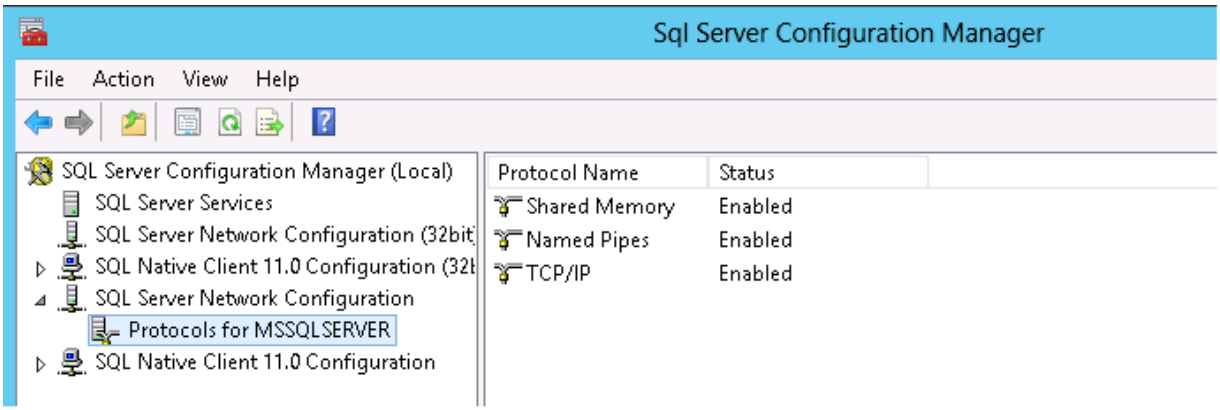
2. If the **SQL Server Browser** service is not started and the **Start** option available in its context menu, it means that this service is disabled. To enable the service, right-click it and from the context menu select **Properties**.



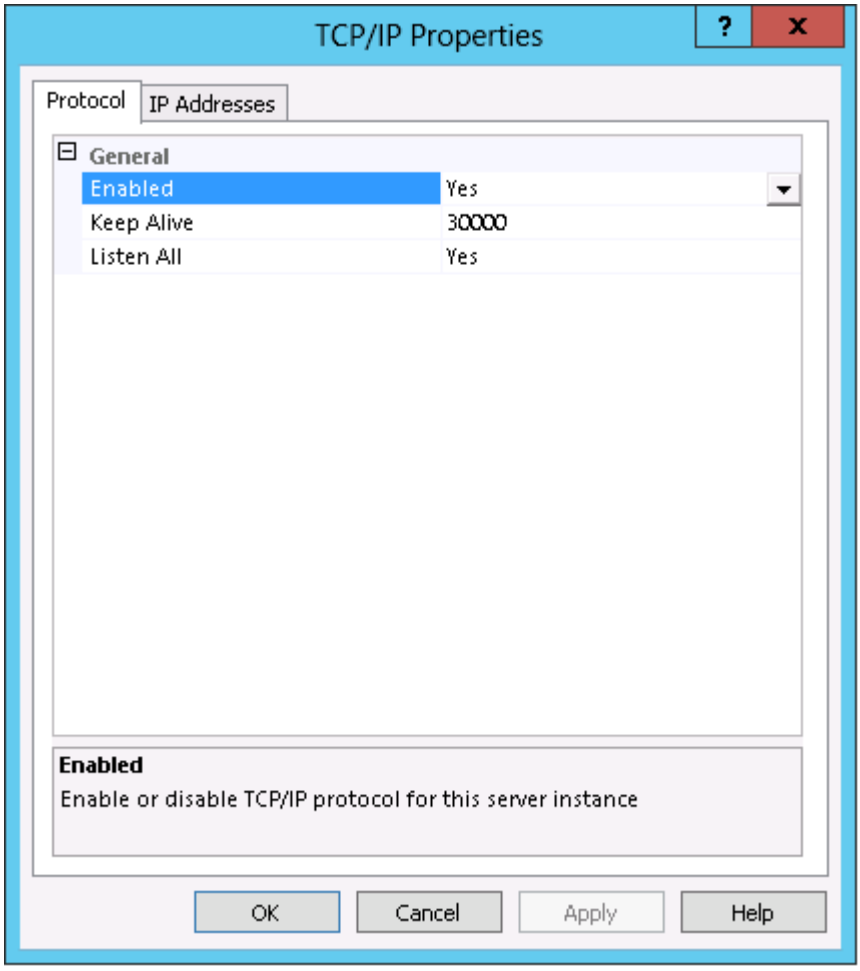
3. The **Properties** window opens. Switch over to the **Service** tab and change the **Start Mode** from **Disabled** to **Manual**. Conclude by clicking **Apply** and **OK** and then try to start the service again.



4. In the **SQL Server Configuration Manager** expand the **SQL Server Network Configuration** node from the navigation tree. On the **Protocols for SQL** node you need to enable the **Named Pipes**, the **Shared Memory** and the **TCP/IP protocols**.

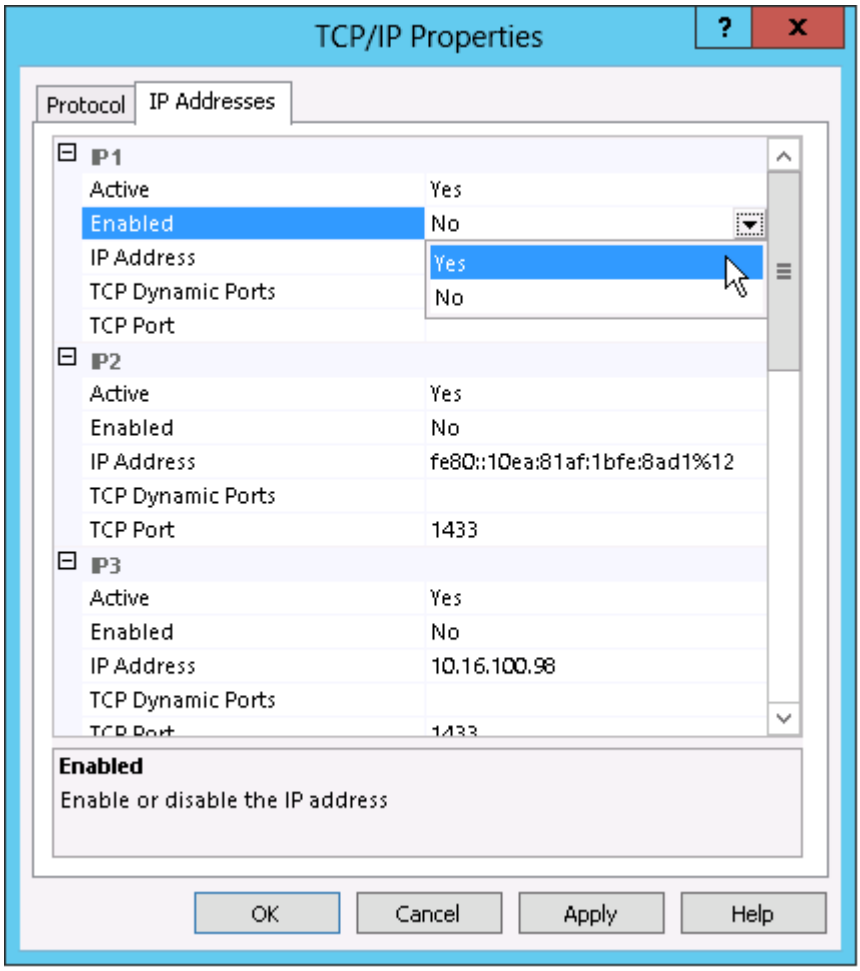


5. Instead of enabling the **TCP/IP** using the context menu, we recommend opening its **Properties** window. This window has two tabs, **Protocol** and **IP Addresses**. On the **Protocol** tab set the **Enabled** to **Yes**.



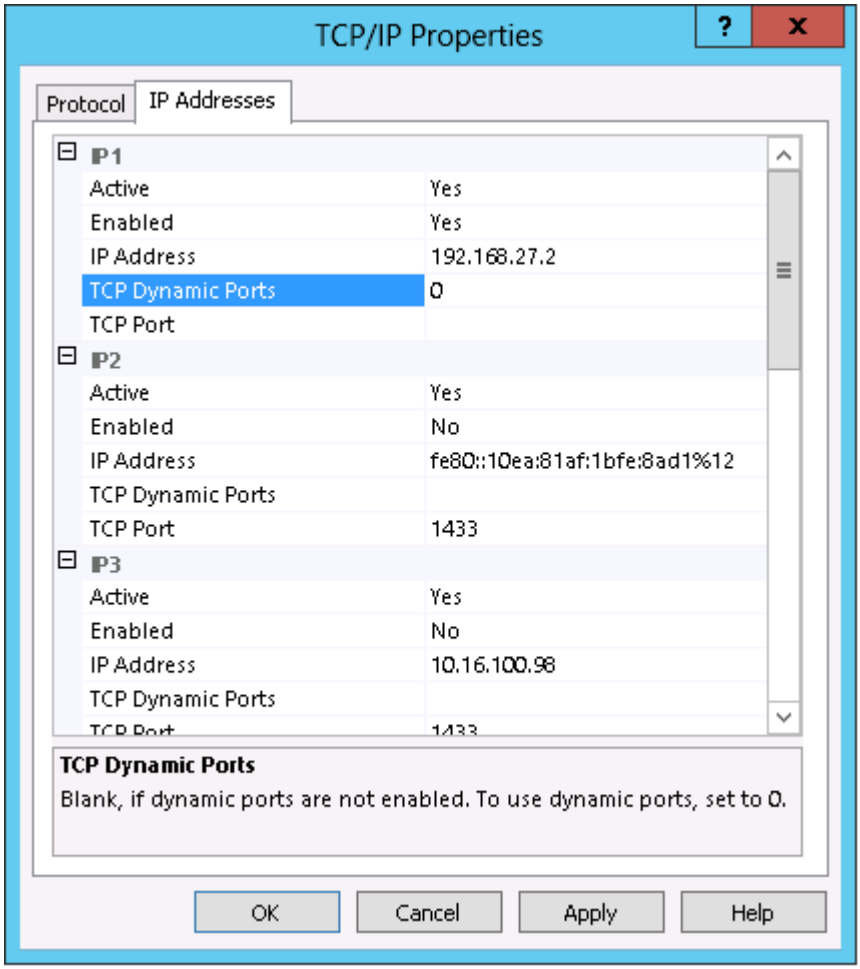
6. On the **IP Addresses** tab you will see several sections - one for each network connection and a local loopback connection indicated by the standard address of 127.0.0.1 For remote access to the SQL Server Express 2012 instance the loopback connection is of no interest.

   For the desired network connection the **Active** option should say **Yes** as should the **Enabled** option. The IP address will probably be filled in for you (by Windows) and will be different on your machine.



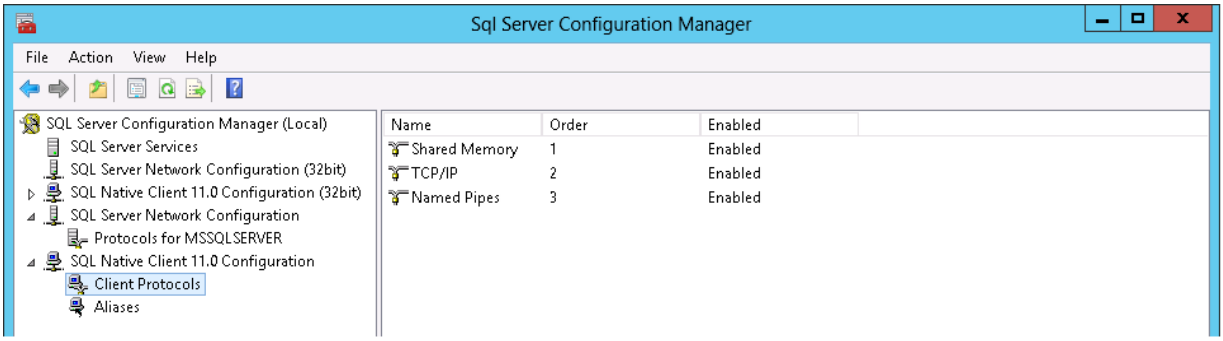
If you wish to enable dynamic ports for your SQL Server Express 2012 instance then the **TCP Dynamic Ports** option should be **0**. To disable this option and use a fixed port change this field to a blank value and fill in the port on the **TCP Port** option. Disabling dynamic ports is non standard for named instances and should really only be done if you know exactly what you are doing and why you want to do it.

Conclude by clicking **Apply** and then **OK**.



7. For the changes to take effect you need to restart both the **SQL Server (SERVERNAME)** and **SQL Server Browser** services have to be restarted switching over to the **SQL Server Services** node.

8. Check the **Shared Memory**, the **TCP/IP** and the **Named Pipes** client protocols on the **SQL Native Client Configuration** node in the **SQL Server Configuration Manager** too. They should all be enabled.

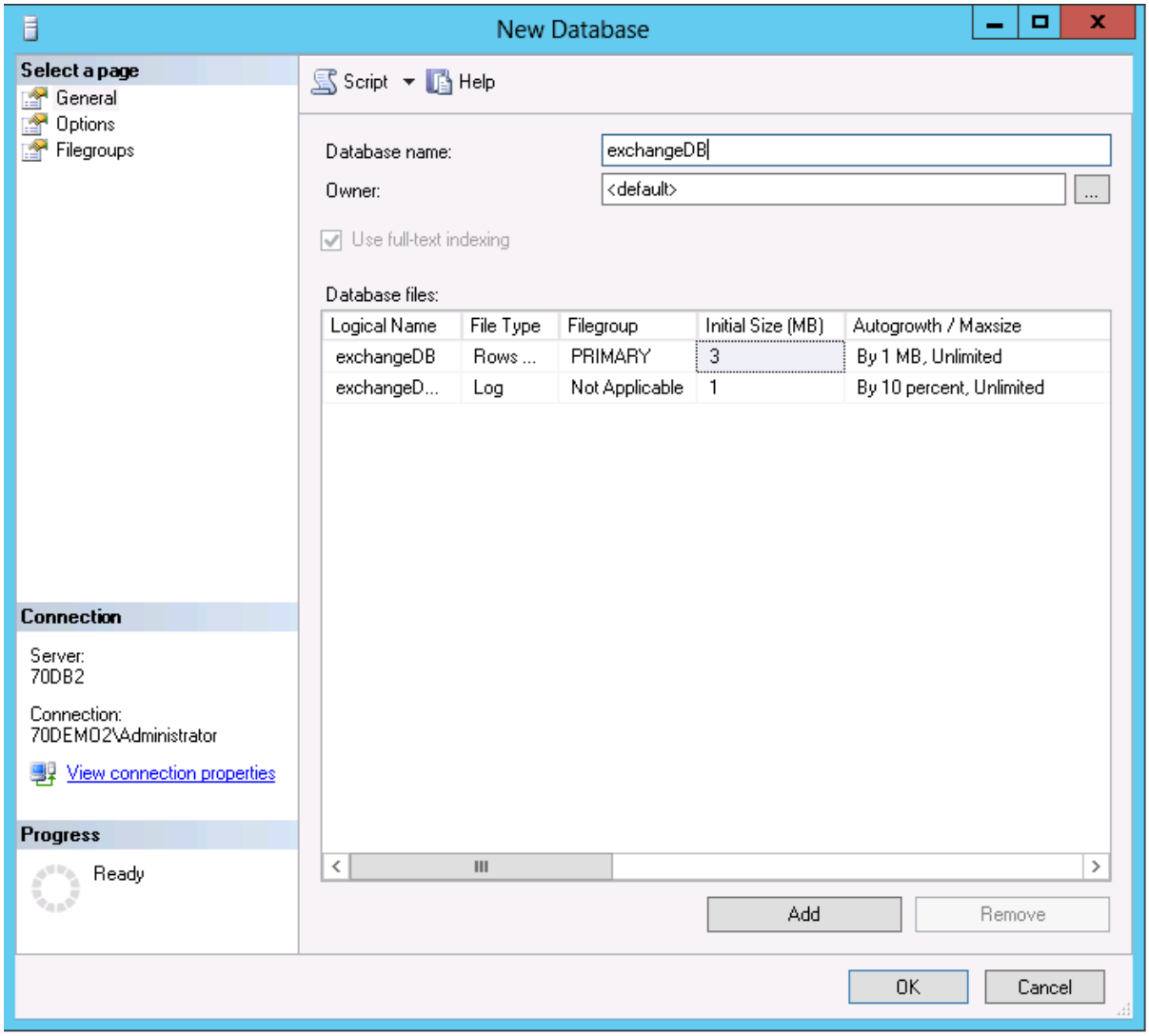


9. Conclude by clicking **Apply** and then **OK**. To apply changes, go to **SQL Server Services** > **SQL Server (<instance_name)** and click **Restart**.

Furthermore you will need to create the empty database and a database user (a SQL Authentication) for your Archive Manager. To do so:

1. Connect to your SQL Server 2012 with the **Microsoft SQL Server Management Studio**, then expand its tree and right-click on the Databases node and choose to create a new database.

2. On the **New Database** dialog, give the new database a name (for instance *exchangeDB*) and you can leave the owner to be the *<default>*. This owner will be changed later on, when you will create a new login with table owner rights over the database you are creating. You can also choose to change the default location for the Data file and Log file, if needed. Conclude by clicking **OK**.

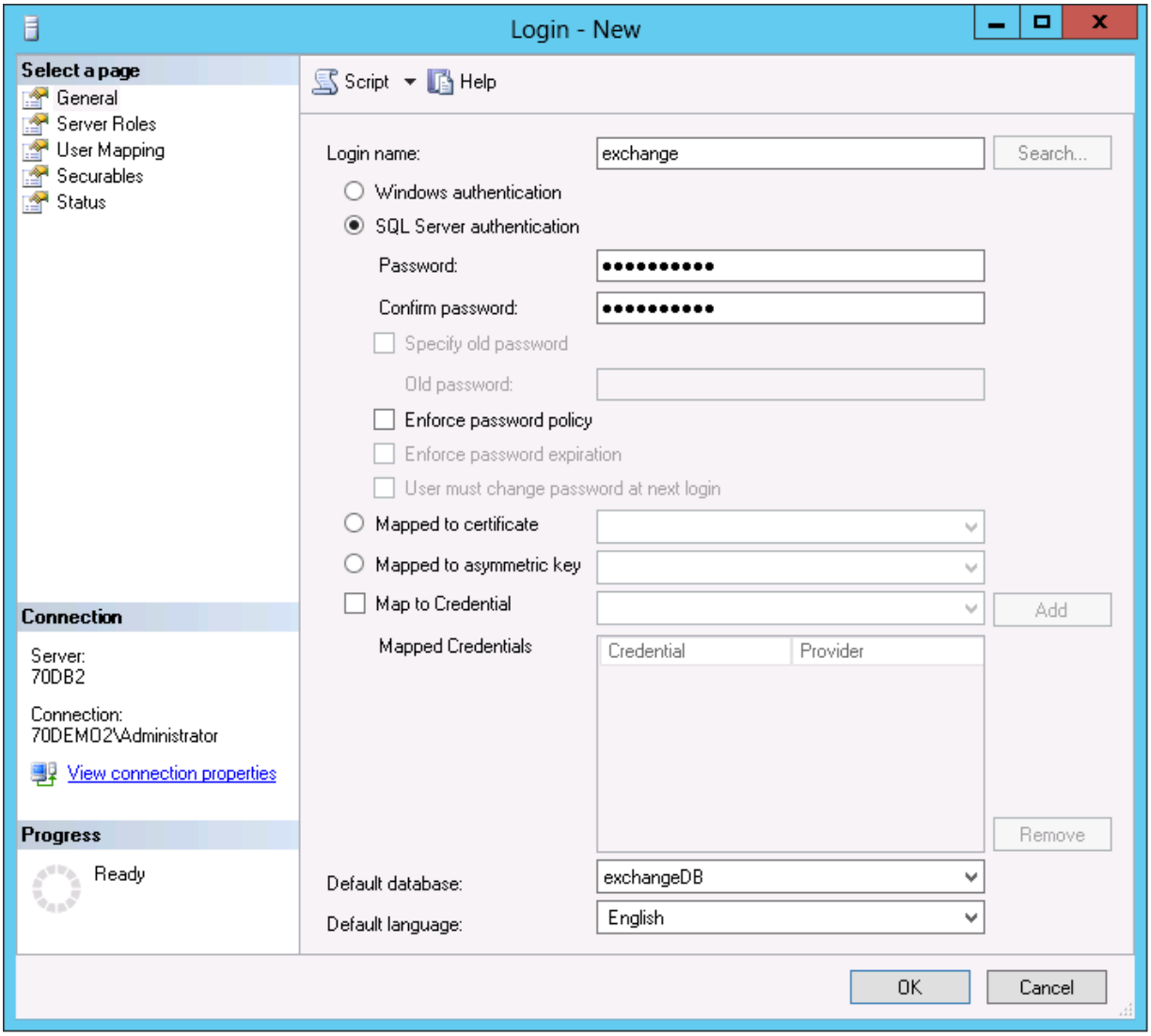


3. To create the Table Owner for the *exchangeDB* database you will need to create a new login, a new scheme and a new user as well. We will name each one of them *exchange*. To create a new login, expand the tree of the **Microsoft SQL Server Management Studio** tool. Right-click on the **Security** tab and choose **New/Login**.

4. The new dialog opens. Before proceeding further on the **General** tab decide on the type of authentication to be used:

   Windows authentication - the user (e.g. “exchange”) must already exist in the Active Directory. Use the **Search** button to find your desired user in AD.

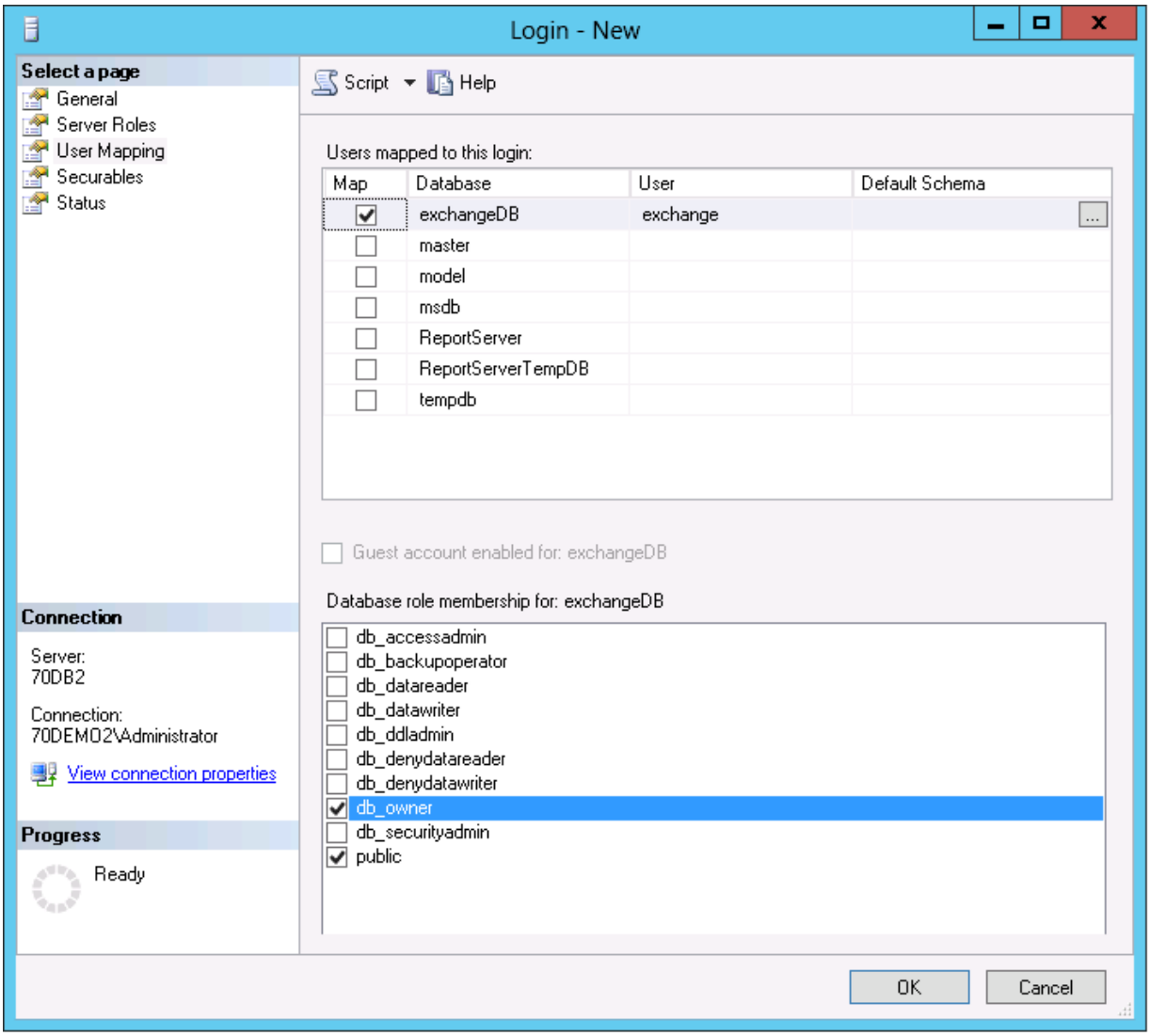
   SQL authentication – specify the login name (“exchange” in our example). Make sure to **uncheck** the **Enforce password policy** check box.



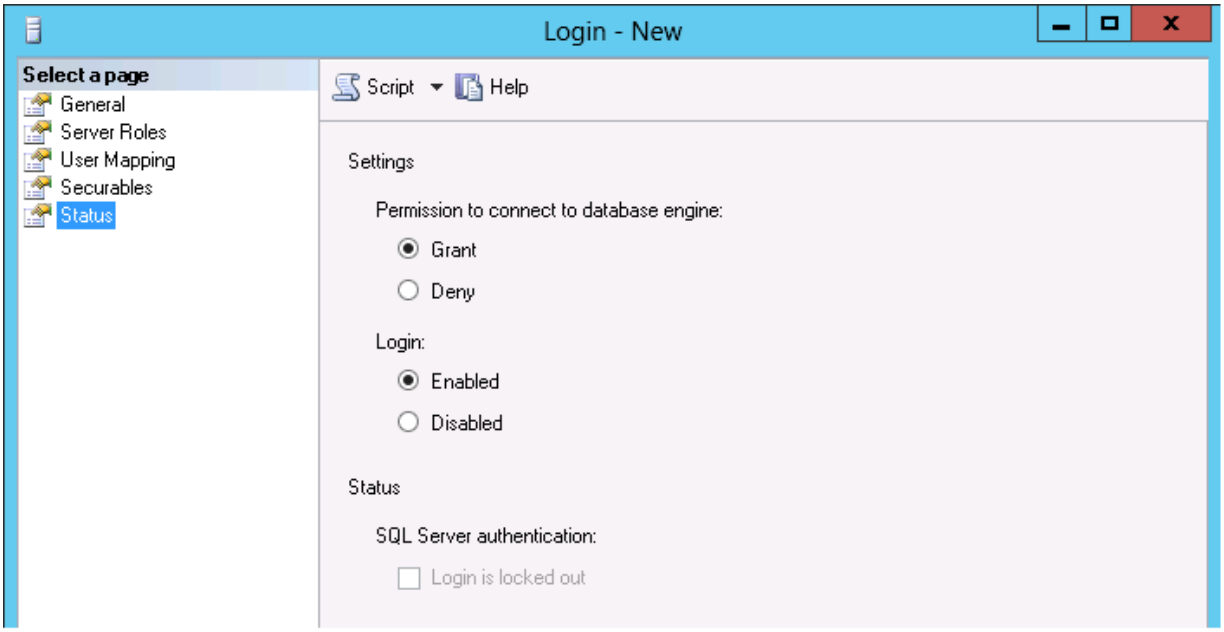
As for the Default database, select the *exchangeDB* database and set the **Default language** to be **English**.

Note: As default the **Enforce password policy**, the **Enforce password expiration** and **user must change password at next login** checkboxes are all selected. You need to make sure that none of them is selected.

5. Once this is done, you can switch over to the **User Mapping** tab. Here map to the *exchangeDB* database a user (it will be automatically created and named with the same name as the login) and select also the **db_owner** and **public** membership role for the *exchangeDB* database.

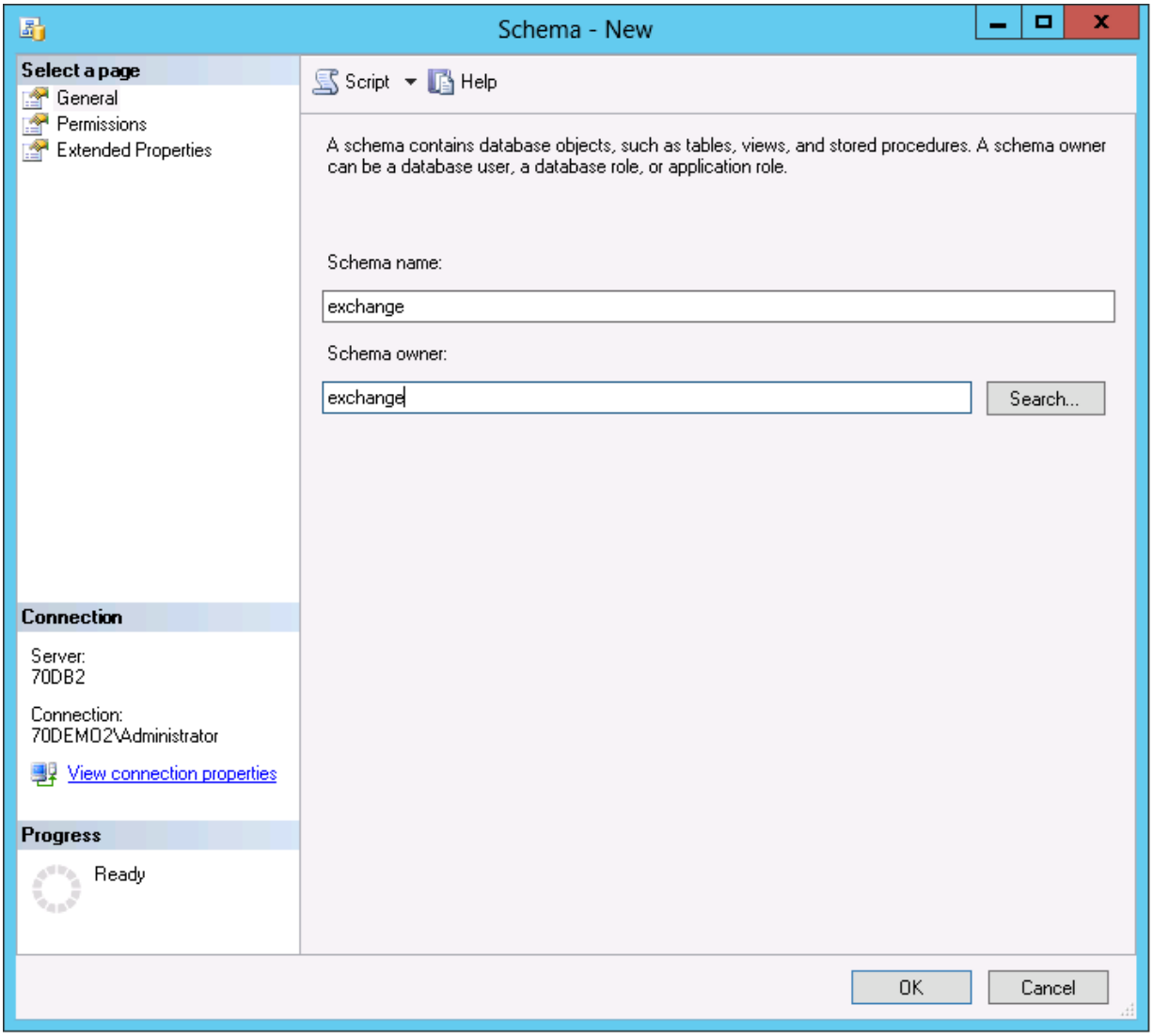


6. Switching over to the **Status** tab make sure the **Permission to connect to database engine** is granted and also that the **Login** is enabled. Conclude by clicking **OK**.



7. Next you will need to create a schema for your new database login. To do so, expand the tree on the new created database (*exchangeDB*) in the **Microsoft SQL Server Management Studio** tool down to **Security/Schemas**. Right-click on **Schemas** and choose **New Schema** from the context menu.

   On the new schema dialog just give a name to the schema you want to create (name it for instance *exchange*) and click the browse button to select the schema owner. Select the schema owner to be the previous user you have specified in step 4 (*exchange*). Conclude by clicking **OK**.



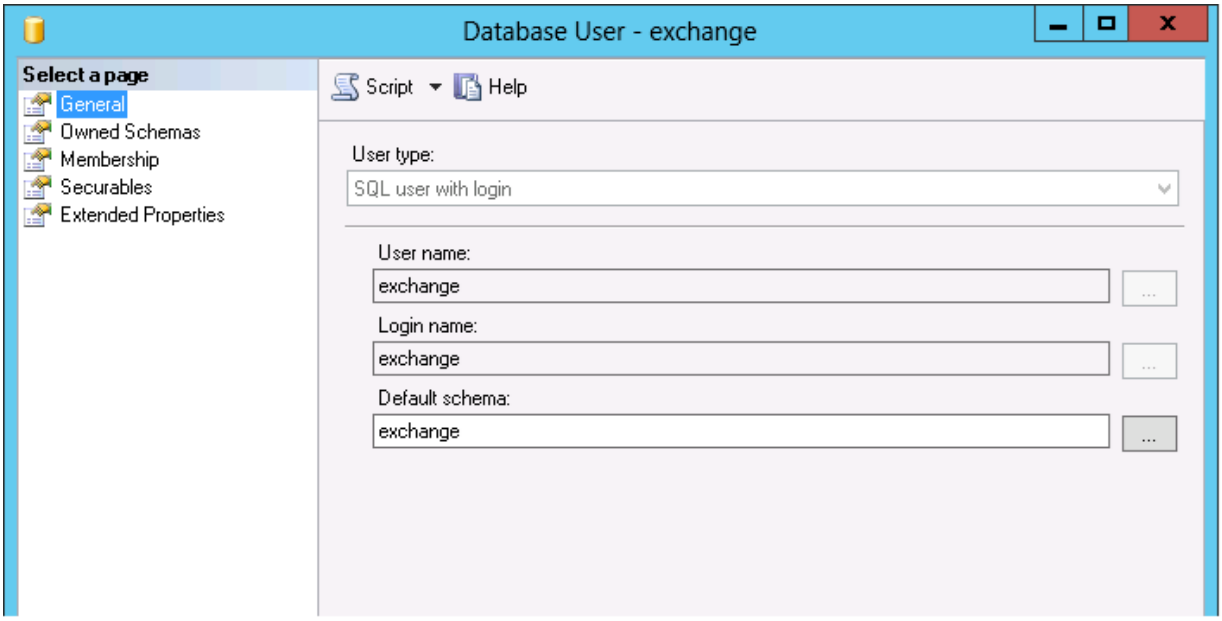
8. Furthermore you will need to assign the new created schema to your new database user. The new database user (*exchange*) was automatically created when creating the new login and mapping a user to the *exchangeDB* database.

   To locate this new user, expand the tree of the *exchangeDB* database in the **Microsoft SQL Server Management Studio** tool down to **Security/Users**.

   By expanding the **Users** node you will see the user called *exchange*.

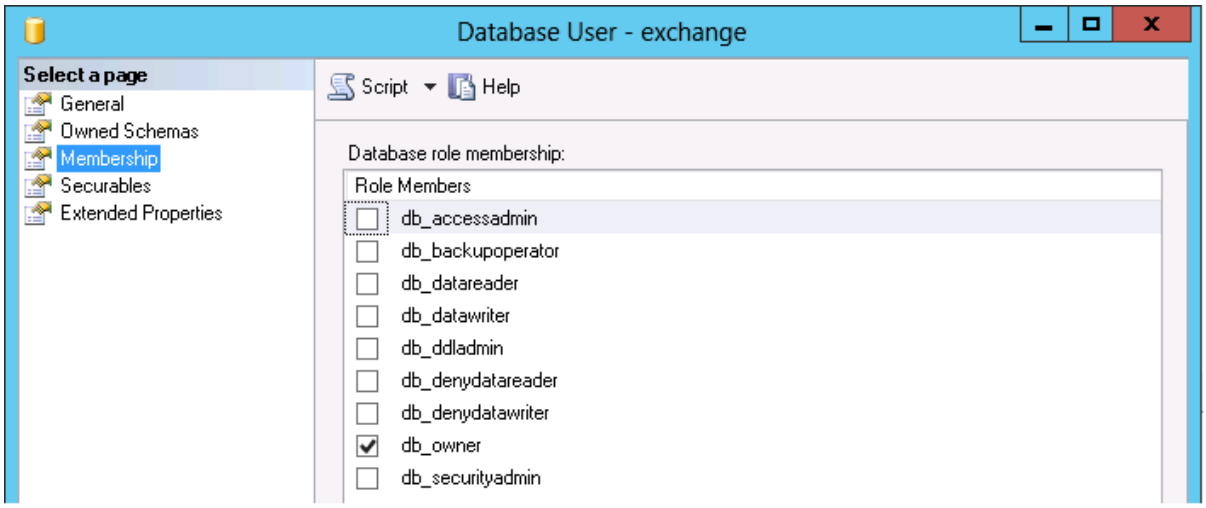
   Double-click on it to open its properties window.

   Click the **General** tab. Here the default schema assigned to your new user is the **dbo** and you will have to replace it to the one previously created (*exchange*) by clicking the browse button.



9. Switch to **Owned Schemas** node where you will see that the one called *exchange* is selected. Make sure that the **db_owner** is selected too.

   Now switch to the **Membership** node and make sure that **db_owner** is selected here, too. Save the changes you have made by clicking **OK**.



At this point we have successfully created one database (*exchangeDB*) with a database user (*exchange*). The database, database user, database-user password and database owner will have to be entered in the database **Configuration** tool.

Remote HSM Server

In case of a remote HSM Server, i.e. if the HSM Server is installed on a separate machine, it is necessary that:

a) the *HSM Base service* runs under the Archive Manager super-user account

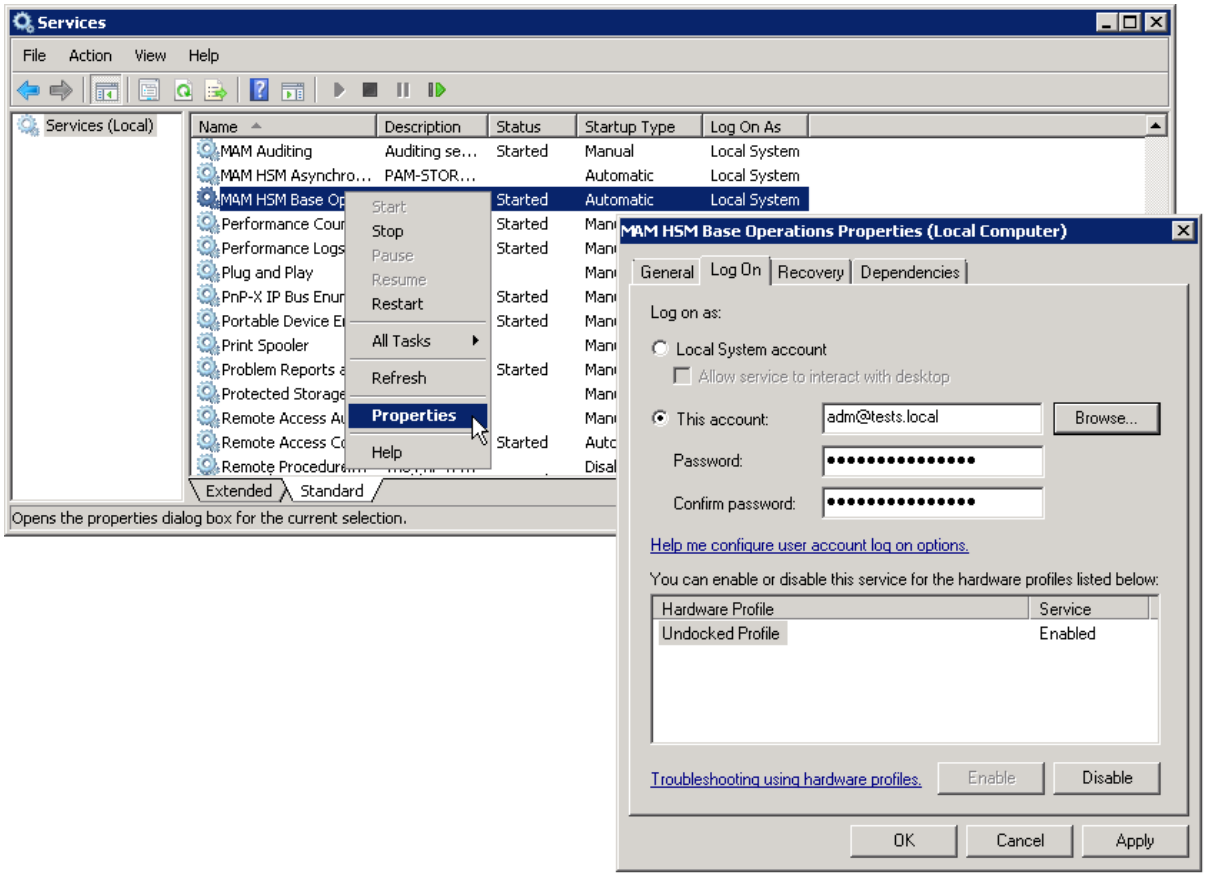
b) DCOM Rights are reduced

a) The Archive Manager super-user account is an account under which our MAM services (MAMfsaHandlerSv, MAMfsaRemoteSV, MAMfsaArchiverSv) run on the Archvie Manager server.

   On the HSM server, follow these steps:

   1. **Open Start / Administrative tools / Services and locate the** *MAM HSM Base Operations* **service.**
   2. **Right-click it and open its Properties. On the Log On tab check This account option and enter the super-user account with its password. (Super-user account is an account which our MAM services** (MAMfsaHandlerSv, MAMfsaRemoteSV, MAMfsaArchiverSv) run under.)

      Finally click **OK**.



b) DCOM Rights has to be reduced in two locations to

AuthenticationLevel="None"

ImpersonationLevel="Anonymous"

and after that the IIS have to be reset.

On the HSM Server follow these steps:

1. **Open machine.config from:**

   C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config

   In case the 64-bit .NET FrameWork open:

   C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config

2. Locate the entry for "processModel" and add:

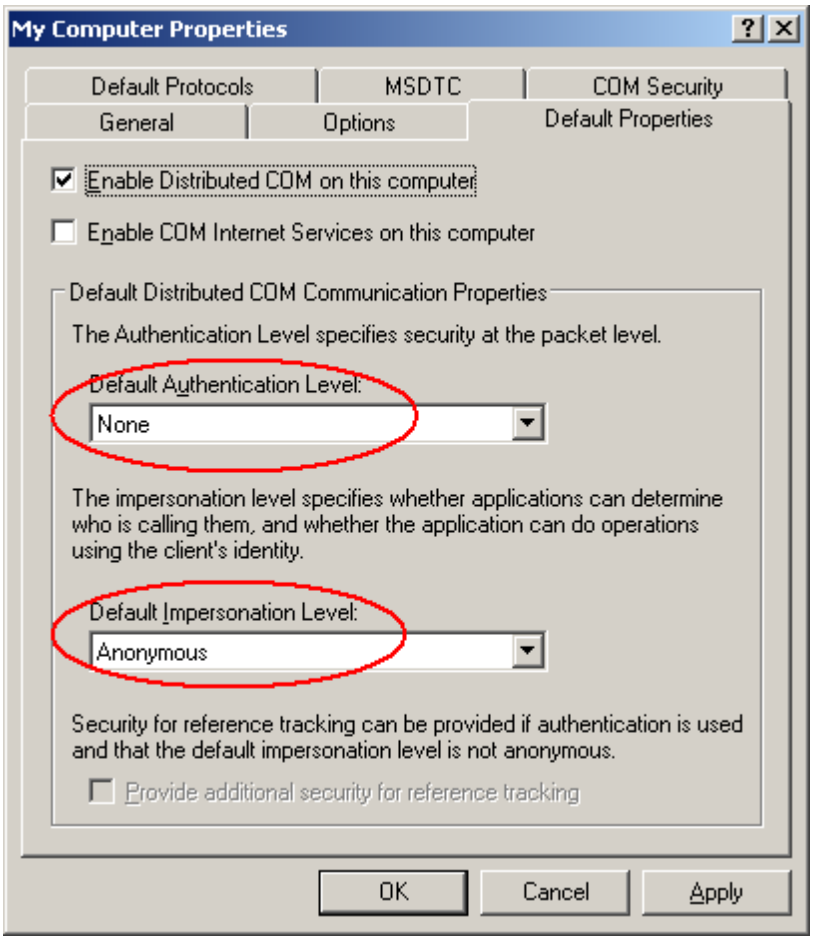
comAuthenticationLevel="None" comImpersonationLevel="Anonymous"

The entry then looks as follows:

```
<processModel autoConfig="true" comAuthenticationLevel="None"
comImpersonationLevel="Anonymous" />
```

3. Close the config.
4. Now run **Component Services** (click **Start /Settings /Control Panel /Administrative Tools /Component Services**).
5. In the **Component Services** window expand the **Component Services** tree down to **Component Services \Computers \My Computer** and then right-click **My Computer** to open its **Properties** window.
6. **Switch over to the Default permissions tab. Check Enable Distributed COM on this computer. Then in the Default Authentication Level dropdown box select None and in the Default Impersonation Level select Anonymous.**

   Click Apply, then OK.



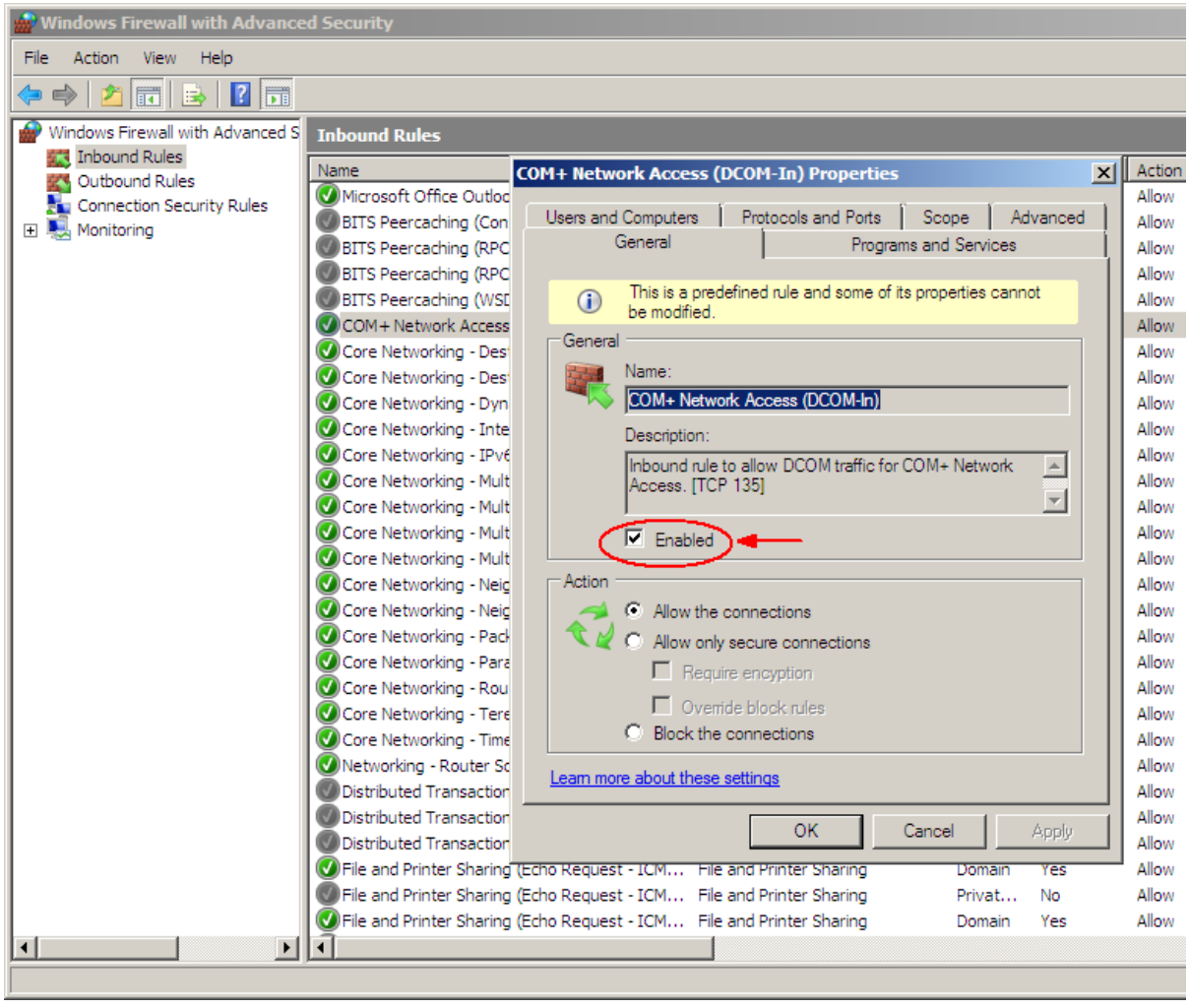
7. **Finally reset IIS.**

HSM configured for Windows Server firewall

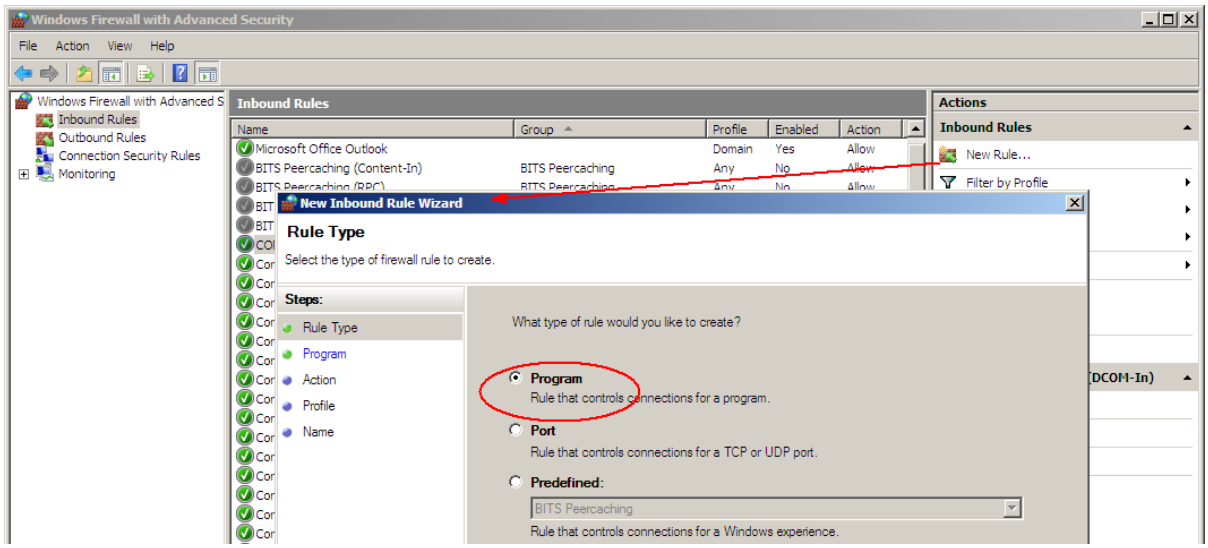
Active Firewall on the **remote** HSM server can cause issues at file retrieving from the archive. To avoid it, the HSM has to be configured properly.

Here are the steps you have to do on Windows Server 2012 / 2016 / 2019 hosting HSM while the Firewall is turned on:

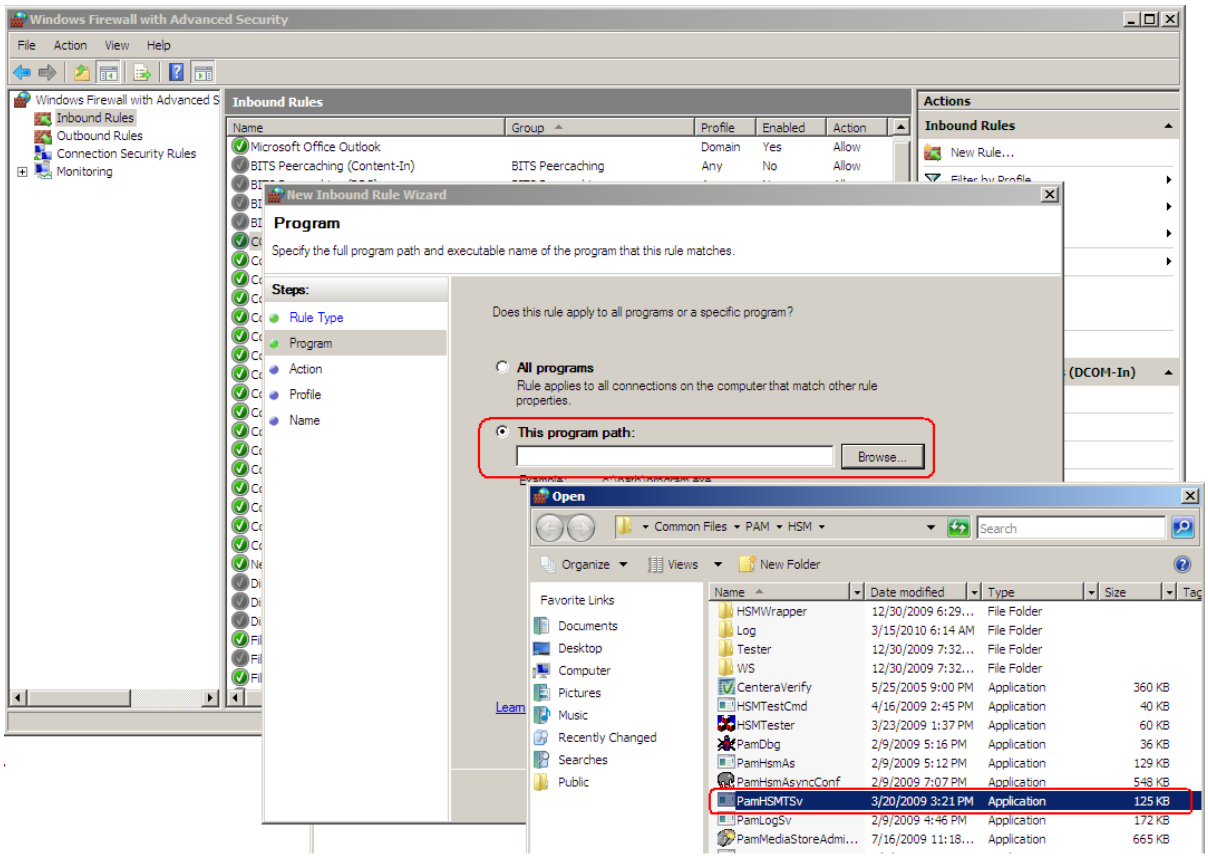
1. You need to allow DCOM traffic for COM+ Network Access. Open Start / Programs / Administrative tools / Windows Firewall. In the **Windows Firewall** under **Inbound Rules** locate COM+ Network Access and right-click it to open its **Properties**. On the **General** tab check **Enable** and then click **OK**.



2. Now create a New Inbound Rule. To do so, click the **New Rule** in the right upper corner. The wizard opens. Select **Program** and click **Next**.

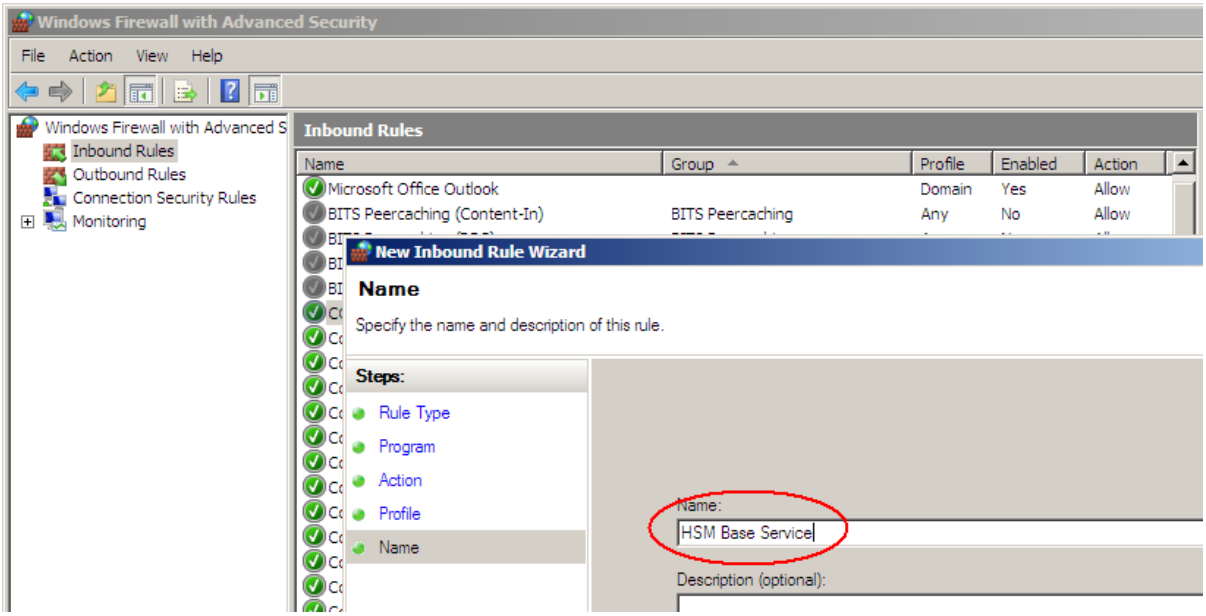


3. On the next page select **This program path** and browse **<installDir>\Common Files\PAM\HSM\PamHSMTSv**. Click **Next**.

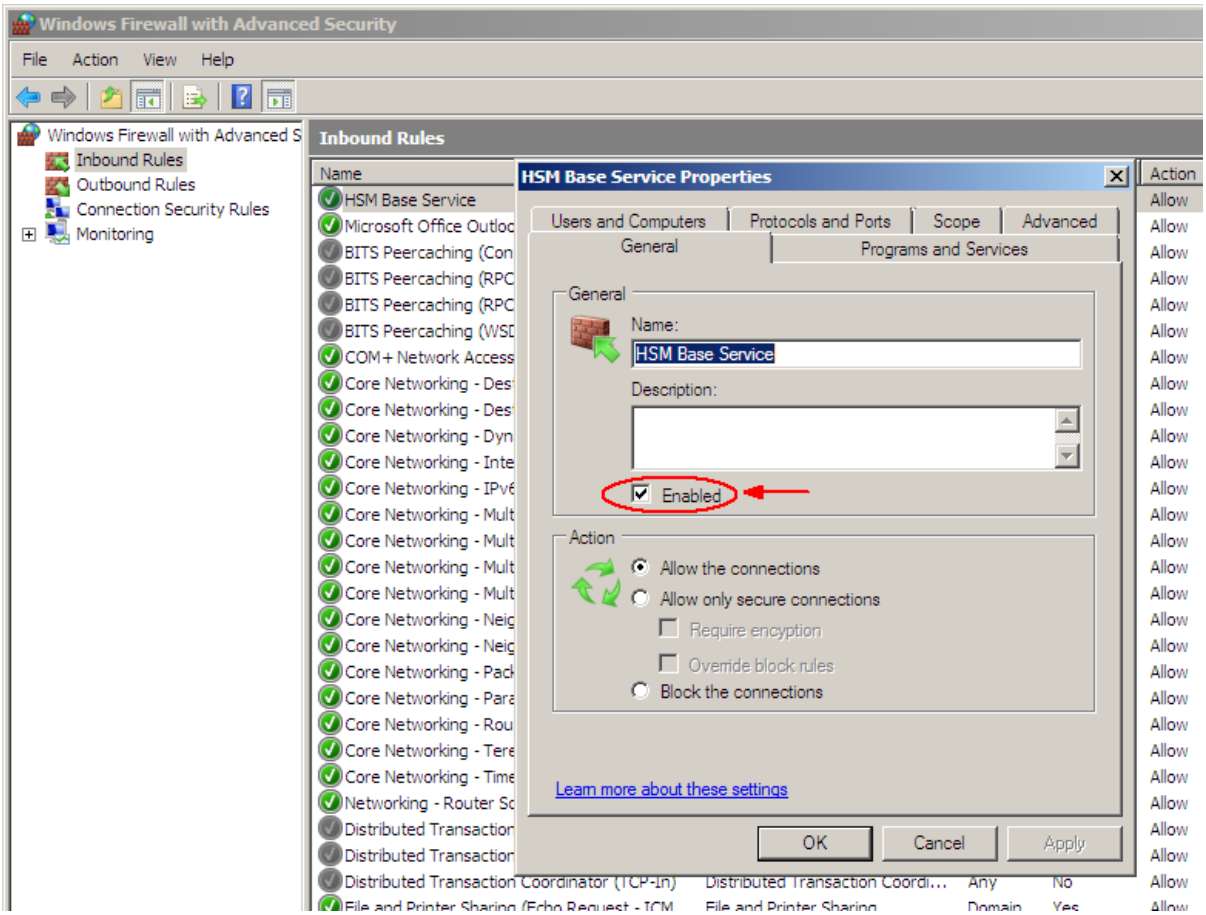


4. Select **Allow the connection** and click **Next**. Then click **Next** again.

5. On the next page name it e.g. **HSM Base Service** and click **Finish**.



6. Open the **Properties** of the new created Inbound Rule and on the **General** tab click **Enable**. Then click **OK**.

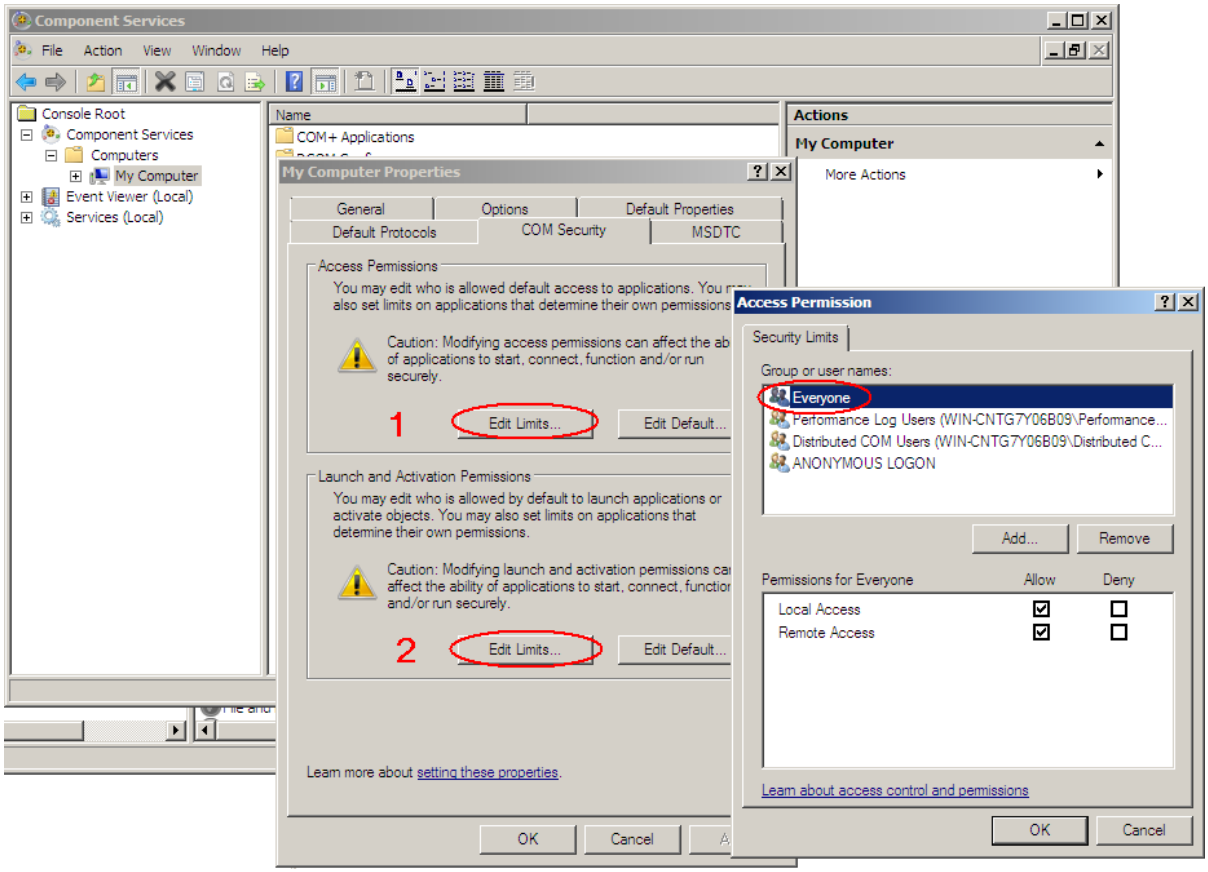


7. Now allow Remote Access and Remote Activation for Everyone in DCOMs. To do so, open **Component Services** (e.g. unfold the tree down to **Component Services** \ **Computers** \ **My Computer**). Open **My Computer Properties**. On the **COM Security** tab:

    - In the **Access Permissions** section click **Edit Limits**. In the pop-up dialog make sure to select **Remote Access** for **Everyone**. Finish by clicking **OK**.

      then

    - In the **Launch and Activation Permission** section click **Edit Limits**. In the pop-up dialog make sure to select **Remote Activation** for **Everyone**. Finish by clicking **OK**.



8. Finally, you can test the connection with HSM tester from the Archive Manager Server.

5

About Us

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

Contacting Quest

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

Technical Support Resources

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

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

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