



Miria Installation Documentation

Miria 4.0

Publication Number: MIRIA-INST-PDF-EN-0223-REV1

Publication Date: February 2023



©2023 Atempo SAS. All rights reserved.

All names and products contained herein are the trademarks or registered trademarks of their respective holders.

The information contained herein is the confidential and proprietary information of Atempo SAS. Unauthorized use of this information and disclosure to third parties is expressly prohibited. This technical publication may not be reproduced in whole or in part, by any means, without the express written consent of Atempo SAS.

Atempo SAS
23 Avenue Carnot
91300 Massy - France

Contents

CHAPTER 1 - Preparing to Install	1
Components	1
Mandatory Components	1
Optional Component: Media Manager	3
Prerequisites to Install	4
Product Download	4
Supported Systems	4
Windows Updates	4
Date and Time	4
Specific Recommendations for Tapes	4
Immutable Disk Repository	5
Environment Resizing	5
Downloading Components	5
Installation Types	6
Installation Modes	6
CHAPTER 2 - Installing Miria Server	8
Before You Install	8
Operating System Prerequisites	8
Secured and Unsecured Access to the Server	9
Installing Server in Graphical Mode	9
Installing the Server in Console Mode	11
Installing the Server in Silent Mode	12
Server Installation Logs	12
Server Services and Daemons	12
Optimizing Linux Installation	13
Switching to an internal or external Database	14
Prerequisites	14
ada_service -switch_data_model command	14
Example of switching from an internal database to an external database	15
Example of switching from an external database to an internal database	15
Creating Several Database Instances	16
ada_service Command	16
Command Syntax	16
Examples for Database Creation on a PostgreSQL Server	18
CHAPTER 3 - Installing Miria Agents	20
Before Installing Agents	20
Installation Requirements	20
Supported Systems	20

Operating System Prerequisites	20
Installing Agents	21
Agent Installation Logs	24
Agent Services and Daemons	24
CHAPTER 4 - Installing Media Manager	26
Installation Prerequisites	26
Windows Library Drivers Update	26
Device Configuration Prerequisites	27
Devices	27
Device Connections	28
Libraries	28
ACSLs Libraries	28
Drives	29
Hardware Recommendations	29
Device Configuration Limitations	29
Installation Parameters	29
Device Configuration	31
Automated Device Configuration	31
Interactive Device Configuration	32
CHAPTER 5 - Updating Miria	37
Update Checklist	37
Update Types	37
Updating in Graphical Mode	37
Updating Components from the CLI	38
CHAPTER 6 - Uninstalling Miria	39
CHAPTER 7 - Use Case #1 - Archiving Data from NAS	40
System Requirements	40
CIFS/SMB NAS	40
Miria	40
Naming	40
Data Flow Diagram	41
Configuring Miria to Archive from NAS	42
Process Overview	42
Connecting to the Administration Console	43
Configuring the Archiving Source	43
Configuring the Archiving Destination	47
Creating the Retention Period	50
Creating the Archiving Policy	51
Creating the Project Archive	53

Creating an Archiving Task	55
Creating the Archiving Task	55
Testing the Archiving Task	57
Archiving and Retrieving Data	58
Archiving Data	58
Retrieving a File	59
CHAPTER 8 - Use Case #2 - Archiving Data to NAS	62
System Requirements	62
CIFS/SMB NAS	62
Miria	62
Naming	62
Data Flow Diagram	63
Configuring Miria to Archive to NAS	64
Process Overview	64
Connecting to the Administration Console	65
Configuring the Archiving Source	65
Configuring the Archiving Destination	68
Creating the Retention Period	72
Creating the Archiving Policy	73
Creating the Project Archive	75
Creating an Archiving Task	77
Creating the Archiving Task	77
Testing the Archiving Task	79
Archiving and Retrieving Data	80
Archiving Data	80
Retrieving a File	81
CHAPTER 9 - Use Case #3 - Archiving Data to Tape Using Media Manager	84
System Requirements	84
Miria	84
Media Manager	84
Naming	84
Data Flow Diagram	85
Configuring Miria to Archive to Tape	85
Process Overview	86
Connecting to the Administration Console	86
Configuring the Archiving Source	87
Configuring the Archiving Destination	89
Creating the Retention Period	95
Creating the Archiving Policy	95
Creating the Project Archive	96
Archiving and Retrieving Data	98

- Archiving Data 99
- Monitoring a Job 100
- Retrieving a File 101
- APPENDIX Migrating the Database from a Version prior to 3.10 105
 - Migration prerequisites 105
 - Upgrading Digital Archive 105
 - Migrating the Digital Archive Database to the New Database Version 106
 - Migrating the Media Manager Database to the New Database Version 106

CHAPTER 1 - Preparing to Install

This topic introduces the Miria components that you must install, and indicates where to install each one. It also describes the installation prerequisites and the Installation Center available on the Miria distribution.

Components

Miria is a client/server application that transfers data between a client or an agent and an archiving server. A specific module then handles access to one or several storage managers, where data is physically copied for its final archiving.

Mandatory Components

This diagram ([Figure 1](#)) shows an environment including a server and several agents:

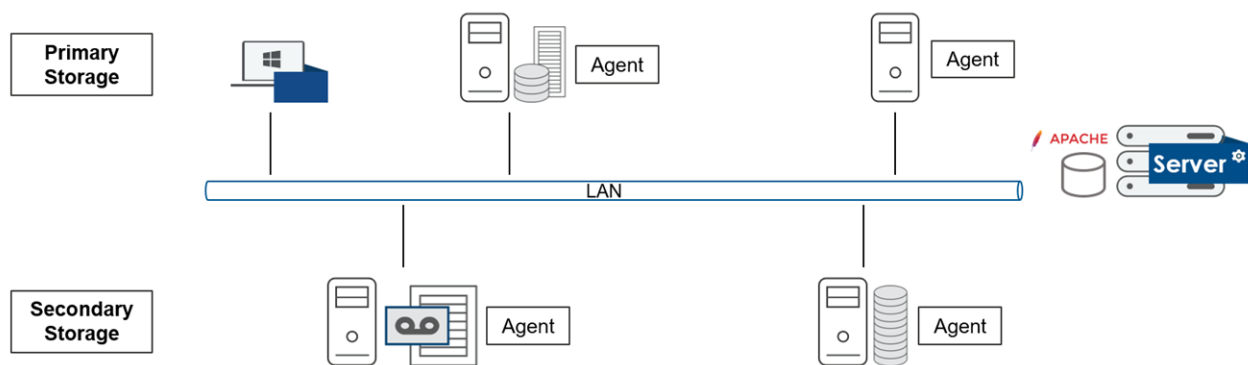


Figure 1: Schematic components overview

You must install these components:

Miria Server




The server manages data transfer onto long-term storage media.

The server:

- Stores information on both the configuration and administration and the archived and retrieved data. Such information is stored in a relational database included in the server installation.
- Manages the scheduling of all automatic tasks, such as automatic archiving or maintenance tasks.
- Manages the network requests from the graphical interfaces.
- Has the agent role (i.e., performs the data movement to and from the secondary storage).

In intensive environments such as medium to large Media & Entertainment configurations or big data configurations, Atempo recommends that you have dedicated agents performing the data movement.

This table describes the server components:

Component	Description
	The Miria engine.
	The relational database is used as a catalog to store configuration, archiving, and retrieval information.
	The Apache server manages network requests using HTTP, HTTPS, and SOAP protocols. It is used by the Web User Interface, Rest API and C API.




Miria Agents

The agent manages data transfers to and from the secondary storage by performing these functions:

- Runs a service to handle requests from the server.
- Handles the writing and reading of data hosted on the platform to which it is related.
- The agent is the data mover component.

Installing an Agent Near the Data Source






You must install agents near the primary storage where the source data to archive is located.

Agent	If the source data is on a:
	<ul style="list-style-type: none"> • Windows or Linux file server. Install an agent on this file server. It handles data reading and transfer to the secondary storage.
	<ul style="list-style-type: none"> • Network Attached Storage (NAS). Install an agent on a platform as close as possible to the NAS. It will act as a Data Mover, handling all data transfers (read, write) to and from the secondary storage.
	<ul style="list-style-type: none"> • Shared file system. Install an agent on any platform having access to the shared file system and that you want to perform the data movement. It is recommended to install several agents if you need fast data movement.

If you are using the Client Archiving feature, the agent component is not needed on the users' workstations. Only a Miria User Interface is required on the computers hosting the files to archive.

Installing an Agent Near the Data Destination

You must install agents near the secondary storage where the data will be archived.

Agent	If the archived data is on a
	<ul style="list-style-type: none"> • Standard file server. Install an agent on this file server. The agent handles data writing and reading to and from the secondary storage.
	<ul style="list-style-type: none"> • Network Attached Storage (NAS). Install an agent on the platform acting as a gateway for the NAS. It handles data writing and reading and transfer to and from the secondary storage.
	<ul style="list-style-type: none"> • Shared file system. Install an agent on any platform having access to the shared file system and that you want to do the data movement. It is recommended that you install several agents if you need fast data movement.
	<ul style="list-style-type: none"> • Media from a tape library administrated by Media Manager. Install an agent together with a Media Manager agent on every machine physically connected to a library or drive. It handles data writing and reading to and from the Media Manager storage manager.
	<ul style="list-style-type: none"> • Cloud/Object Storage/CAS. Install an agent on the primary storage where the source data is located.

See [Installing Miria Agents](#) for details.

Administration Console

The Administration Console provides administration and supervision. From this console, you manage settings for the entire system, including enabling license keys, managing and configuring the storage, creating users and groups, and managing the archiving policies. You can also use it as a power User Interface to archive or retrieve data locally.

For more information on the administration functions, see the Administrator Documentation.

Miria User Interface

The User Interface enables end users to archive, search, and retrieve their own files.

See the Miria User Documentation for details.

Optional Component: Media Manager

Media Manager is a storage manager used by Miria to archive data directly to tape and manage the media. Install this optional component if you want to archive your data for long-term protection on a tape library.

Media Manager is composed of:

- A Media Manager server, which manages requests coming from the Media Manager agents and assigns media to Miria.
- Media Manager agents, which manage libraries and drives.

See the Administrator Documentation for details.

Where to Install Media Manager

You must install each component in the appropriate location:

- The Media Manager server on the Miria server.
- A Media Manager agent on every machine physically connected to a library or drive, together with a server or agent. This component is lightweight; it requires a negligible amount of CPU and RAM.

See [Installing Media Manager](#) for details.

Prerequisites to Install

Before installing Miria, take into account these prerequisites:

Product Download

Ensure that you have downloaded the binaries from the [Atempo Client Portal](#).

Supported Systems

The list of supported operating systems for each component is subject to frequent evolutions. For the most up-to-date information, see the [Miria Compatibility Guide](#) at the Atempo Website.

Windows Updates

Important: The Windows Updates automatic reboots may put your archiving production at risk, especially if they occur when a scheduled task is due or while jobs are in progress. Ensure that the Windows Update process does not automatically restart the platforms hosting Miria components.

Date and Time

The scheduling system requires that each platform used is on time and configured according to its local time zone.

Specific Recommendations for Tapes

- **FC Card Port.** In a Windows or Linux environment, *do not* use only one port for the Disk and the Tape/Library. You must ensure that you have, at least, one dedicated port for the disk and one dedicated port for the tape or library.
- **Drivers.** Follow these recommendations:
 - For LTO, use only the generic driver.
 - For T10K on Windows, use Oracle T10K driver.
 - For T10K on Linux, use the `st` Linux generic driver.
- **LTO-7 and Windows 2012 R2**
If you plan to use IBM LTO-7 and Windows 2012 R2, you must apply the appropriate Microsoft hotfix.

- **Atempo Recommendations.** To achieve the best performances, follow these recommendations:
 - Assign at least 2 GB for the datamovers.
 - Do not use the multi-path feature for the tape or the library.
 - According to throughput expected, use a dedicated FC (Fiber Chanel) card for Disk or Tape/Library.
 - Use a dedicated Miria/Media Manager server with no connection to Primary Storage and no connection to Library/Drive.
 - Ensure that datamovers have a connection to Disk and Library/Drive.

Immutable Disk Repository

Immutable disk repository is based on a Linux machine, featuring immutable flag compatible file system (xfs or ext3/ext4).

You need to upfront provision such partition if you want to use this feature.

Important: It is mandatory to correctly secure the root account of this machine.

Environment Resizing

If you need to resize your existing archiving environment, ensure to meet these prerequisites on all Miria servers and agents performing data movement:

- **Memory.** If you plan to significantly increase the number of files archived, you must upgrade the memory in proportion.
For instance, if you expect to double the number of files archived, you must double the memory too (e.g., upgrade the memory from 64 GB to 128 GB).
- **CPU.** Upgrade the CPU in these situations:
 - If you plan to ingest a large quantity of metadata through a third-party application (e.g., Avid Interplay), XML Ingest, etc.
 - If you need servers and/or agents to perform partial retrieval.

If you need additional help or guidelines to resize your hardware configuration, contact Atempo Professional Services.

Downloading Components

1. Log in to the [Atempo Client Portal](#).
2. Enter your credentials.
3. Click the **Download** tab. The list of available productversions is displayed.
4. Select the version that you want to download. It is composed of several **.zip** files:
 - **Server** Contains a single installer for Server (including web user Interface), Agent, and Media Manager (Server and Agent).
 - **Admin** Graphical administration console for Windows only.
5. Click the **Download** link corresponding to your Operating System and processor architecture.
6. Copy on your platform the **.zip** file containing the executable binaries.

7. Unzip the `.zip` file to obtain the executable binaries.

You can now install the component:

- Miria Server installation details: see [Installing Miria Server](#)
- Miria Agent installation details: see [Installing Miria Agents](#).
- Miria Media Manager: see [Installing Media Manager](#).

Installation Types

There are two types of installations available: **Typical** and **Custom**. The following components are always installed:

- Miria engine.
- Database. New installations are PostgreSQL only for all Operating Systems. If you upgrade an existing installation with MaxDB, you will be using MaxDB in the upgraded version.
- Apache Web Server.

The typical installation includes a pre-selection of the most commonly used parameters with the following default settings:

- Home path:
 - **Windows** `C:\<DEFAULT_PATH>` for the server and `C:\Program Files\<DEFAULT_PATH>` for agents.
 - **macOS** `/Applications/Miria`
 - **Linux** `/Miria` or `dt/prod/Miria`.
- TCP/IP port: `2524`
- HTTP Apache port `80` and/or HTTPS Apache port `443`

A custom installation enables you to install Media Manager as an optional component.

Check the following table to verify the availability of Miria components for each operating system.

Operating system	Miria Server	Miria Agent	Media Manager Server	Media Manager Agent
Windows	Yes	Yes	Yes	Yes
Linux	Yes	Yes	Yes	Yes
macOS	No	Yes	No	No

Installation Modes

Miria server, agents and Media Manager can be installed using one of the following installation modes.

- **Graphical mode** Use the step-by-step graphical wizard installation. Refer to the installation chapter of each Miria component.

- **Console mode** Use the step-by-step wizard installation in interactive command-line interface. You can use this mode when there is no GUI environment on the server. See also [Installing the Server in Console Mode](#).
- **Silent mode** Automate the installation process without user interaction. See also [Installing the Server in Silent Mode](#).

Before you perform the installation, check the table below to verify the installation modes available for your operating system.

Operating system	Graphical mode	Console mode	Silent install
Windows	Yes	Yes	Yes
Linux	Yes	Yes	Yes
macOS	Yes	No	No

CHAPTER 2 - Installing Miria Server

This chapter explains how to install Miria Server interactively or in silent mode. It includes useful information that enables you to understand the server component.

Before You Install

See [Prerequisites to Install](#) for general prerequisites and hardware requirements.

Operating System Prerequisites

To ensure that Miria server works correctly, your operating system must meet these requirements:

Platform	Requirement
Windows	No requirement.
Linux	<p>Installation requires some packages to be installed before running the installer.</p> <p>For an installation in CLI using console mode or silent mode, run these commands to install required packages:</p> <ul style="list-style-type: none"> • DEB-based distributions <code>apt-get update && apt-get install -y --no-install-recommends psmisc gawk</code> • RPM-based distributions <code>yum update && yum install psmisc gawk</code> <p>For an installation in graphical mode, run these commands to install required packages:</p> <ul style="list-style-type: none"> • DEB-based distributions <code>apt-get update && apt-get install -y --no-install-recommends psmisc gawk libxext6 libxtst6 libxrender1 fontconfig fonts-dejavu</code> • RPM-based distributions <code>yum update && yum install psmisc gawk libXext libXtst libXrender fontconfig dejavu-sans-fonts dejavu-serif-fonts</code> <p>Note: For Centos 8 or superior, run also the following command to install the required package: <code>yum install glibc-all-langpacks</code></p> <p>Installation in graphical mode requires a graphical environment (X Windows) on the local host or a DISPLAY variable set to use graphical environment from a remote host.</p>

Secured and Unsecured Access to the Server

By default, Miria uses HTTPS; however, you can configure the Miria server to accept both HTTP and HTTPS connections.

It is recommended to use only secured protocol (HTTPS) for all communications with the server.

Installing Server in Graphical Mode

- > Launch the **Installation Wizard** in the manner corresponding to your operating system. This table lists the available operating systems:

Operating System	Launch Actions
Windows	<p>Run the <code>installMiria.exe</code> program.</p> <p>On systems with User Account Control (UAC) enabled (e.g., Windows 2008 R2), a control dialog box prompts you to approve the program installation, and may require you to enter an administrator's password.</p>
Linux	<p>Open a shell and <code>cd</code> to the directory where you downloaded the installer.</p> <p>At the prompt:</p> <ol style="list-style-type: none"> 1 Extract the installation setup by running this command: <pre>tar xvfz installMiria.tgz</pre> 2 Launch the installation setup by running this command: <pre>sh ./installMiria.bin</pre>

This table describes the parameters that you can enter in the Installation Wizard to perform a server installation:

Parameter	Options and Actions
License Agreement	Carefully read the general licensing conditions in their entirety and then select I accept the terms of the License Agreement .
Installation Type Selection	Select Server .

Parameter	Options and Actions
Choose Install Set	<p>These are the valid options :</p> <ul style="list-style-type: none"> • Typical Recommended for most users. • Custom Installation with customized features. <p>Note: If the installation Wizard detects a Miria database, it warns you that it will update the Miria server. See Administrator Documentation to backup your Miria database.</p> <p>Click Next for the setup to update the Miria server.</p>
Choose Install Folder	<p>Select the path for the installation.</p> <p>The default path is entered automatically, but you can change it. Manually enter a new path or click Choose to open the Select a Folder window and browse your network to find a new destination folder.</p>
Optional Components	<p>For a Custom installation only.</p> <p>Depending on the operating system, the installation wizard enables you to install the Atempo Media Manager (Windows, Linux).</p>
Miria Server	<p>Displays these read-only information fields for Typical installation:</p> <ul style="list-style-type: none"> • Environment Name ADA • Miria Server Name <localhost> (i.e., the machine on which you are currently installing Miria). • Port 2524.
Miria Communication Ports	<p>This port enables the Miria interfaces to communicate with the Miria server.</p> <p>Select the check box for one or both of these options:</p> <ul style="list-style-type: none"> • HTTP Port Provides unencrypted access to the server at login. The default port number is 80, but if this is already in use, you can choose another port. • HTTPS Port Provides encrypted access to the server at login. The default port number is 443, but if this is already in use, you can choose another port. <p>See Secured and Unsecured Access to the Server for details on access ports.</p>

Parameter	Options and Actions
Install Media Manager	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Do not install AMM Component The Setup does not propose to install Media Manager. • Install AMM Agent The Setup installs a Media Manager agent. See Media Manager - Agent Installation. • Install AMM Server (contains an agent) The Setup installs a Media Manager server. See AMM Installation - Server Installation.
Miria Database (PostgreSQL)	<p>For a Custom installation only.</p> <p>Enter a port for the Miria database.</p> <p>This is a PostgreSQL database, which uses the default listening port <code>5433</code>.</p> <p>Modify the port number, if necessary.</p>
Optional Components	<p>For a Custom installation only.</p> <p>Enter the information required for the Media Manager component. See also Installing Media Manager.</p>
Firewall Configuration	<p>This window opens only if the firewall is enabled on your system. The behavior of this window depends on the operating system:</p> <ul style="list-style-type: none"> • Windows and Linux RedHat Configure the firewall to open the Miria ports. Choose <code>Yes</code> for the firewall to be automatically configured. • Linux SUSE It detects the firewall presence, but does not configure it. A message indicates that you must manually open the firewall to the Miria ports.
Pre-Installation Summary	Review the installation parameters and click Install to launch the installation.
Install Complete	Displays the Installation exit status.

Installing the Server in Console Mode

If the server cannot be installed in graphical mode, you can use the command line interface (CLI) to perform the installation interactively. It is identical to the installation wizard and takes you step-by-step through the different sub-installations.

> To use the console mode, run the installer in CLI and add the `i-console` parameter.

Example: On Linux, launch `sh installMiria.bin -i console`.

Installing the Server in Silent Mode

The silent mode can be used to automate the installation process. This installation mode requires no user interaction.

The setup for your operating system contains a sample file (`silent_install.txt`). This file includes a complete description of installation and update parameters.

There are three commands to run the silent installer. This depends on how the values are set for the required installation parameters. Each option is outlined below.

To run the silent setup with all default values

> Launch `installMiria.bin -i silent`.

To run the silent setup with specified installation parameters

The silent setup will be done with specified installation parameters set in the `silent_install.txt` sample file. Use a bare metal text editor to customize and rename this file or to create a new file.

1. Make a copy of the sample file and save it as a text file.
2. Set the value of the required installation parameters. These are indicated in the parameter's header section of the sample file. By default, `INSTALLATION_TYPE` is set to install the Server component.
3. Save your changes.
4. Open a command window and go to Miria installer directory.
5. Verify that the directory contains the file that you created.
6. Launch `installMiria.bin -i silent -f silent_install.txt`.

To run the silent setup with default values except for the value provided

> Launch `installMiria.bin -i silent -DOPTION1=X -DOPTION2=Y`. Option names and values are detailed in the `silent_install.txt` file.

Server Installation Logs

The installation log files for the server are stored in this Miria installation directory path:

- **Windows.** `Miria\Uninstall\Install_Logs`
- **Linux and macOS.** `Miria/Uninstall/Install_Logs`

Server Services and Daemons

The server installation sets up and starts these services:

Operating System	Services and Daemons
Windows	<p>These are the Windows services:</p> <ul style="list-style-type: none"> • ADA:Apache2 • ADA:Server Engine • PostgreSQL (or MaxDB when upgrading an existing installation): ADA
Linux	<p>These are the Linux services:</p> <ul style="list-style-type: none"> • Apache server. • Miria server engine. <p>The ADA_ADA script, located in the /etc/init.d directory, automatically launches this service at every server machine reboot.</p> <ul style="list-style-type: none"> • PostgreSQL engine (or MaxDB when upgrading an existing installation) <p>The ADADB_ADA script, located in the /etc/init.d directory, automatically launches this service at every server machine reboot.</p>

Optimizing Linux Installation

The installation on Linux creates in the <ADA_HOME>/Tools/tuning installation directory these configuration files :

- `linux_sysctl.txt`.
 - For RedHat 7.x, using the `root` account, copy this file in the `/etc/sysctl.d/50-ADA.conf` directory.
 - For RedHat 5.x/6.x, using the `root` account, append this file (`append` command) to `/etc/sysctl.conf` file.
- `limits.conf`. Increases the number of files that a process can open.

To enable the `limits.conf` file

1. Using the `root` account, open the `/etc/security/limits.conf` file in a text editor.
2. At the end of the file, add these two lines:

```
* hard nofile 65536
```

```
* soft nofile 16384
```

3. Save the `/etc/security/limits.conf` file.
4. Run this command:

```
sysctl --system
```

If you experience problems enabling the `linux_sysctl.txt` and `limits.conf` files, turn off the firewall by running these commands:

- RedHat 6.x.

```
service iptables stop
```

```
checkconfig iptables off
```

- RedHat 7.x.

```
systemctl stop firewalld
```

```
RedHat 5.x/6.x. systemctl disable firewalld
```

Switching to an internal or external Database

By default, during Miria's installation, a PostgreSQL database is installed on the Miria server. This database can be switched to another PostgreSQL server for better integration into the existing infrastructure. The CLI allows the database switch and only changes all references in order to provide Miria with new connection settings. These settings are used to connect to another PostgreSQL server.

This section describes how to switch from a PostgreSQL internal database to a PostgreSQL external database or vice versa.

Prerequisites

- Prior to the database switch, the Miria database content must be migrated to the PostgreSQL external server or vice versa. You can use the `create_data_model` option to initialize a new database (BETA).
- The external PostgreSQL user must have a **Superuser** status. Otherwise, the `create_data_model` command will fail.
- PostgreSQL should be installed on the external machine before switching databases.
- PostgreSQL must be installed with the `tablefunc` module (available in the [contrib library](#)).
- The PostgreSQL server must be reached through the port provided in the Miria server.
- The database on the destination server must have the same name as the database on the source server.

ada_service -switch_data_model command

To switch from a PostgreSQL internal database to a PostgreSQL external database, use the following command:

```
ada_service -switch_data_model -db_admin_identity {Name:Password} -db_name {Name} -db_port {Port} -db_hostname {hostname} [-db_ssl_mode {prefer|disable|allow|require} ] Switch between internal and external Postgres data model
```

This table describes the options that you can use with this command:

Option	Description
<code>-db_admin_identity</code>	Specifies the login and password of the administrator of the target PostgreSQL database (example: postgres:postgres).

Option	Description
<code>-db_name</code>	Specifies the name of the source PostgreSQL database.
<code>-port</code>	Specifies the communication port for the target PostgreSQL server.
<code>-db_hostname</code>	Specifies the name of the target machine.
<code>-db_ssl_mode</code>	Specifies the TCP/IP connexion is SSL-secured. The authorized values are <code>prefer</code> <code>disable</code> <code>allow</code> <code>require</code> .

Example of switching from an internal database to an external database

In this example, an external PostgreSQL external database is used:

- Machine name: `serverpg`
- Port: `5438`
- User db_admin: `postgres`
- Password db_admin: `postgres`
- Database name: `ADA`

To switch to an external database

1. Run the command:

```
ada_service -switch_data_model -db_admin_identity postgres:postgres -db_name
ADA -db_port 5438 -db_hostname serverpg
```

A confirmation dialog containing a summary of the selected parameters appears : **Connection to external DB successfully, SSL:off, mode:prefer**

2. Confirm that you want to switch to an external PostgreSQL database.
3. Specify the host, database name, port and admin user for the target database. In this example:
 - Host: `serverpg`
 - DB Name: `ADA`
 - Port: `5438`
 - Admin user: `postgres`

A confirmation dialog is displayed when the database switched successfully.

Example of switching from an external database to an internal database

In this example, a PostgreSQL internal database is used:

- Machine name: `localhost`
- Port: `5433`
- User db_admin: `postgres`

- Password db_admin: `postgres`
- Database name: `ADA`

To switch to an internal database

1. Run the command:

```
ada_service -switch_data_model -db_admin_identity postgres:postgres -db_name ADA -db_port 5433 -db_hostname localhost
```

2. Confirm that you want to switch to an internal PostgreSQL database.
3. Specify the host, database name, port and admin user for the target database. In this example:
 - Host: `localhost`
 - DB Name: `ADA`
 - Port: `5433`
 - Admin user: `postgres`

A confirmation dialog is displayed when the database switched successfully.

Creating Several Database Instances

The Typical and Custom setups install a database that stores information related to Miria administration, archiving, and retrieval.

The setup creates only one database instance called `ADA`. However, once the Miria server is installed, you can easily create additional database instances that you can use as testing databases, for example.

When logging on to the Administration Console, you can select the database to which you want to connect. An external template can be generated.

ada_service Command

The `ada_service` command enables you to create, list, and delete database instances. The `ada_service` command must be run on the Miria server.

The Miria binaries are located in the `ADA_HOME/Binary/Bin` directory. You or the user `root` can run them from a command terminal after navigating to this directory.

- **Windows.** It is safer to use the Environment Prompt, which ensures that all proper environment variables are set:
Select Start › All Programs › Miria › Miria Environment Command Prompt.
- **Linux.** Open a terminal in the `ADA_HOME/Binary` directory and set the Miria environment by running this command:

```
. .ADA.sh
```

Command Syntax

To create an additional instance, use this command syntax:

```
ada_service -create_data_model -db_admin_identity Login:password -db_name
dbname -db_type MaxDB|Postgres [-db_portportnb]
```

To list the data models, use this command syntax:

```
ada_service -list_data_model
```

To delete an instance, the `root` user can use this command syntax:

```
ada_service -delete_data_model -db_name dbname -identity root:password
```

This table describes the options that you can use with the `ada_service` command:

Option	Description
<code>-create_data_model</code>	<p>Creates an additional instance to the Miria database.</p> <p>Once the instance is created, a line describing the instance is added to the <code>\$ADA_HOME/Binary/Conf/ada_servers</code> file:</p> <pre>DBName [HostName] [User] [Password] [DataBaseType] [DBName] [Schema] [Port] [Connect_ Options]</pre> <p>Names of databases should be unique. You cannot create a new database using the same name as an existing one. This rule applies to both internal and external databases.</p>
<code>-delete_data_model</code>	<p>Enables the <code>root</code> user to delete the specified instance from the existing database.</p> <p>Prerequisites to use the <code>-delete_data_model</code> option:</p> <ul style="list-style-type: none"> • Can only be run in the Miria server. • The <code>root</code> user cannot delete the instance of the database if it is the only one existing in the Miria configuration. Trying to delete the database unique instance exits the command on error and displays the <code>Default DB cannot be deleted</code> message. • No jobs must be running on the concerned database. <p>Once the instance is deleted, Miria removes the line that describes the instance from the <code>\$ADA_HOME/Binary/Conf/ada_servers</code> file.</p>
<code>-db_admin_identity</code>	<p>The user must have the necessary rights to create databases.</p> <p>This option is available in beta version.</p>
<code>-db_name dbname</code>	<p>The <code>-db_name</code> option specifies:</p> <ul style="list-style-type: none"> • For the <code>-create_data_model</code> option, the name of the database instance to be created. • For the <code>-delete_data_model</code> option, the name of the data instance to be deleted.

Option	Description
<code>-db_type</code> <code>MaxDB Postgres</code>	<p>The <code>-db_type</code> option is mandatory and specifies the database type.</p> <p>Windows and Linux. Creates a PostgreSQL database (or MaxDB for upgrades of an existing installation only).</p>
<code>-identity</code> <code>root:password</code>	Specifies the root user identity, that is mandatory to use the <code>-delete_data_model</code> option.
<code>-list_data_model</code>	<p>Lists the data models defined in the <code>ada_servers</code> file.</p> <p>This option provides this information for each data model:</p> <ul style="list-style-type: none"> • DB Name (logical name) • Host Name • User • DataBase Type • DB Name (instance) • Schema

Examples for Database Creation on a PostgreSQL Server

This topic includes two examples on how to create a new database on an internal or external PostgreSQL server.

Note: Names of databases should be unique. You cannot create a new database using the same name as an existing one. This rule applies to both internal and external databases.

The path for the `ada_servers` file is different for each OS:

- Windows `..\Miria\Binary\Conf\`
- Linux `../Miria/Binary/Conf/`

Creating a New Database on an Internal PostgreSQL Server

```
ada_service -create_data_model -db_admin_identity postgres:postgres -db_name
ADATEST -db_type postgres -db_port 5432
```

A line is automatically added to the `ada_servers` file describing the newly created instance:

- Database admin identity: postgres:postgres
- Database name (logical name): ADATEST
- Type: PostgreSQL
- TCP Port: 5432

Creating a New Database on an External PostgreSQL Server

```
ada_service -create_data_model -db_admin_identity postgres:postgres -db_name
serverpg:ADATEST -db_type postgres -db_port 5432
```

A line is automatically added to the `ada_servers` file describing the newly created instance:

- Database server: serverpg

- Database admin identity: postgres:postgres
- Database name (logical name): ADATEST
- Type: PostgreSQL
- TCP Port: 5432

CHAPTER 3 - Installing Miria Agents

This topic describes the typical and custom installations of Miria agents.

Before Installing Agents

Before installing the agents, read carefully this information.

Installation Requirements

To ensure that agent works correctly, your system must have at least 2 GB of disk space.

See [Prerequisites to Install](#) for general prerequisites.

Supported Systems

The list of supported operating systems for each component is subject to change often; for the most up-to-date information, see the [Miria Compatibility Guide](#).

Operating System Prerequisites

To ensure that the agent works correctly, your operating system must meet these requirements:

Platform	Requirement
Windows	No requirement.

Platform	Requirement
Linux	<p>Installation requires some packages to be installed before running the installer.</p> <p>For an installation in CLI using console mode or silent mode, run these commands to install required packages:</p> <ul style="list-style-type: none"> • DEB-based distributions <code>apt-get update && apt-get install -y --no-install-recommends psmisc gawk</code> • RPM-based distributions <code>yum update && yum install psmisc gawk</code> <p>For an installation in graphical mode, run these commands to install required packages:</p> <ul style="list-style-type: none"> • DEB-based distributions <code>apt-get update && apt-get install -y --no-install-recommends psmisc gawk libxext6 libxtst6 libxrender1 fontconfig fonts-dejavu</code> • RPM-based distributions <code>yum update && yum install psmisc gawk libXext libXtst libXrender fontconfig dejavu-sans-fonts dejavu-serif-fonts</code> <p>Installation in graphical mode requires a graphical environment (X Windows) on the local host or a DISPLAY variable set to use graphical environment from a remote host.</p>
macOS	<p>In the <code>/etc/sysctl.conf</code> file, Miria automatically modifies the configuration values for the shared memory:</p> <ul style="list-style-type: none"> • <code>kern.sysv.shmmax=524288000</code> • <code>kern.sysv.shmall=131072000</code>

Installing Agents

The Miria distribution includes an installation Wizard, which takes you step-by-step through the installation of each component. This procedure is outlined below.

Note: If you want to install agents interactively or in silent mode from the command line interface, see [Installation Modes](#).

You must install the agent in the appropriate location, depending on your configuration:

- On the file servers where the files to archive are located.
- If you are using the File Storage storage manager, on the platforms where the files are archived.
- If the files are located on an NDMP file server (NAS), on a platform that acts as a gateway to the NAS.

On macOS (in the `/etc/sysctl.conf` file), Miria automatically modifies the configuration values for the shared memory:

- `kern.sysv.shmmax=524288000`
- `kern.sysv.shmall=131072000`

To install agents in graphical mode

- > Launch the Installation Wizard in the manner corresponding to your operating system.

Operating System	Launch Actions
Windows	<p>Run the <code>installMiria.exe</code> program.</p> <p>On systems with User Account Control (UAC) enabled (e.g., Windows 2008 R2), a control dialog box prompts you to approve the program installation, and may require you to enter an administrator's password.</p>
macOS	<p>After downloading the installer, double-click <code>installMIRIA</code>.</p> <p>A dialog box informs you that you need Administrator-level rights to perform the installation. Enter the password and click OK.</p>
Linux	<p>Open a shell and <code>cd</code> to the directory where you downloaded the installer.</p> <p>At the shell prompt:</p> <ol style="list-style-type: none"> 1 Extract the installation setup by running this command: <pre>tar xvfz installMiria.tgz</pre> 2 Launch the installation setup by running this command: <pre>sh ./installMiria.bin</pre>

The agent installation parameters are described in the table below.

Parameter	Options and Actions
License Agreement	Carefully read the general licensing conditions in their entirety and then select I accept the terms of the License Agreement .
Installation Type Selection	Select Agent (Storage Node) .
Choose Install Set	<p>These are the valid options :</p> <ul style="list-style-type: none"> • Typical Recommended for most users.. • Custom Installation with customized features.
Choose Install Folder	<p>Select the path for the installation.</p> <p>The default path is entered automatically, but you can change it. Manually enter a new path or click Choose to open the Select a Folder window and browse your network to find a new destination folder.</p>
Optional Components	<p>For a Custom installation only</p> <p>Depending on the operating system, the installation wizard enables you to install Media Manager (Windows, Linux, macOS).</p>

Parameter	Options and Actions
Miria Agent	<p>Enter the required parameters:</p> <ul style="list-style-type: none"> • Environment Name If the environment used is Miria, this field displays <code>Miria</code> and cannot be modified. If Miria is not used, this field lets you enter manually the name of your environment. • Miria Server Name Server name or IP address to which the agent must connect. Enter your server name or IP address. <p>Automatic Detection Mode</p> <ul style="list-style-type: none"> • Automatic Detection If you select this button, the Setup performs tests to autodetect the port and the logical name that the Miria server uses to communicate with the agents. The Setup gets this information from the values you entered in the Miria Server Name and HTTP/HTTPS Port fields. • HTTP/HTTPS Port TCP/IP Port through which the Miria agent requests to the Miria server the port number they must use to communicate together. Enter the same port number as the one you defined at server installation. The default value for HTTP port is <code>80</code>, and for HTTPS port is <code>443</code>. • Use SSL encryption If you select this check box, the requests from the agent to the server are encrypted (SSL encryption). <p>If you want to install the agent even if your server is not running, select the Manual Setting button to switch to the manual setting.</p> <p>Manual Setting</p> <ul style="list-style-type: none"> • Manual Setting If you select the Manual Setting button, the Setup does not perform any tests. Instead, it uses the values you entered in the <code>Miria Server Name</code> and <code>Miria Server Port</code> fields. • Miria Server Name Enter your server name or IP address. Ensure that the name is <i>identical</i> to the name specified for the server at the installation time. The name is case-sensitive and the agent cannot connect to the server if there is any discrepancy. To get the exact server name, on the machine hosting the server run the <code>ada_service -get_ada_info</code> command. For more information on this command, see the Administrator Documentation. • Miria Server Port The default value is <code>2524</code>. Enter the same port number that the server uses to communicate with the agents.

Parameter	Options and Actions
Optional Components	<p>For a Custom installation only</p> <p>Enter the information required for the Media Manager component. See also Installing Media Manager.</p>
Install Media Manager	<p>It eases the Media Manager server or agent installation. These are the valid options:</p> <ul style="list-style-type: none"> • Do not install AMM Component The Setup does not propose to install Media Manager. • Install AMM Agent The Setup installs an agent. See Media Manager - Agent Installation. • Install AMM Server (contains an agent) The Setup installs a server. See AMM Installation - Server Installation.
Firewall Configuration	<p>This window opens only if the firewall is enabled on your system. The behavior of this window depends on the operating system:</p> <ul style="list-style-type: none"> • Windows and Linux RedHat Configure the firewall to open the Miria ports. Choose Yes for the firewall to be automatically configured. • Linux SUSE It detects the firewall presence, but does not configure it. A message indicates that you must manually open the firewall to the Miria ports.
Pre-Installation Summary	Review the installation parameters and click Install to launch the installation.
Install Complete	Displays the Installation exit status.

Agent Installation Logs

The installation log files for the agents are stored in this Miria installation directory path:

- **Windows.** `Miria\Uninstall\Install_Logs`
- **Linux and macOS.** `Miria/Uninstall/Install_Logs`

Agent Services and Daemons

The Miria agent installation sets up and starts these services:

Operating System	Services and Daemons
Windows	The <code>ADA:Agent Engine</code> service is set up and started at the Miria agent installation.

Operating System	Services and Daemons
macOS	<p>The service created after Miria Agent installation is:</p> <pre>ada_daemon (/Applications/Miria/Binary/Bin/ada_daemon -launch)</pre>
Linux	<p>The Miria agent engine. This is launched automatically at every reboot of the agent machine with the script <code>ADA_ADA</code> found in the <code>/etc/init.d</code> directory on SUN Solaris and Linux.</p> <p>The service created after Miria agent installation is:</p> <pre>ada_daemon (/Miria/Binary/Bin/ada_daemon -launch)</pre>

CHAPTER 4 - Installing Media Manager

Media Manager is an optional component that you can install with Miria.

Installation Prerequisites

Before you install Media Manager, ensure to meet these prerequisites:

- You must install libraries and/or drives and declare them in the operating systems of the machines physically connected to the devices.
- You must perform SAN zoning before you install Media Manager components.
Ensure that SAN/TAPE and SAN/DISK are in different SAN zones.
- **Windows.**
 - Update the library drivers.
 - Stop the Removable Storage Windows (NtmsSvc) service.
If this service is started, some conflicts may occur for media access.
 - If you install Media Manager in a directory called Program Files (e.g., C:\Program Files), ensure that there is no other file or directory named program at the same root (e.g., C:\Program).
The Media Manager services cannot start correctly because Media Manager uses a PostgreSQL database that has a known limitation in handling blank spaces in file or directory names.

Windows Library Drivers Update

On a Windows system, before configuring a library, you must update the system driver to avoid any detection issue. The only system driver supported is *Unknown Medium Changer*.

Important: If the Windows Update program suggests a Hardware Update and you select the option to update the library driver, this will restore the vendor driver and undo the corrective process described above. Media Manager will then no longer work until you reset the library driver to Unknown Medium Changer.

To update the system driver

1. From the **Windows Desktop**, right-click **My Computer** and select **Manage**.

The **Computer Management** window appears (Figure 2):

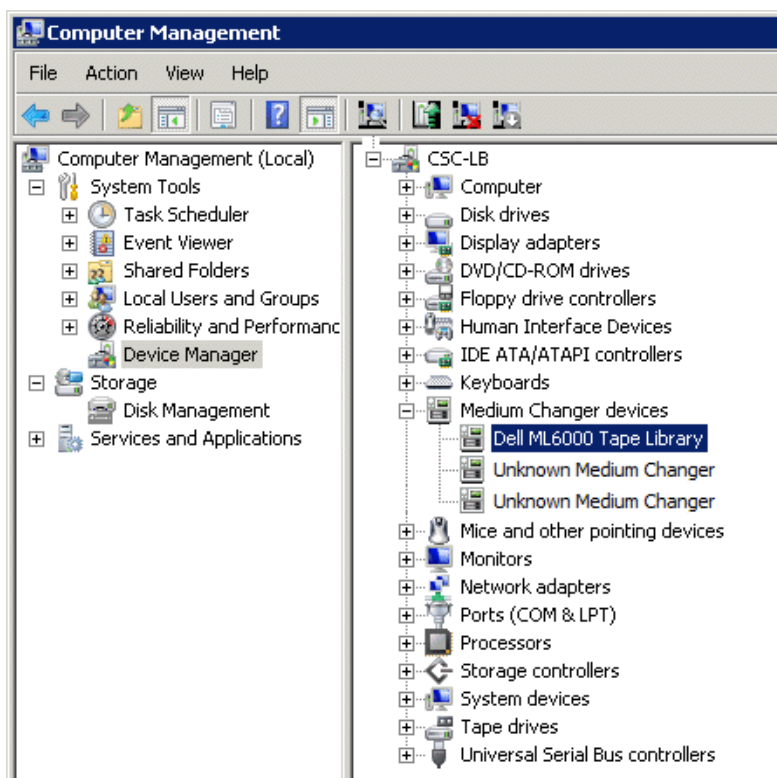


Figure 2: Computer Management window

2. On the left pane, expand the **System Tools** node, then click **Device Manager**.
3. On the right pane, double-click **Medium Changer devices**.
4. Ensure that no library vendor driver is configured for libraries.
Unknown Medium Changer must be the only driver under the Medium Changers node. If vendor drivers are listed, remove them.
 In the sample screen, you must remove the **Dell ML6000 Tape Library**.
5. Right-click the vendor driver and select **Update Driver Software** to open the wizard.
6. In the **Welcome** screen, click **Browse my computer for driver software**.
7. In the **Search** screen, click **Let me pick from a list of device drivers on my computer**.
8. In the **Device Selection** screen, select **Show Compatible Hardware** and select **Unknown Medium Changer** from the list of compatible hardware, then click **Next**.
9. Exit the wizard.

Device Configuration Prerequisites

The list of supported operating systems and devices is subject to frequent changes. For the most up-to-date information, see the [Miria Compatibility Guide](#).

Devices

These are the device prerequisites:

- You can only use Media Manager with devices reporting a serial number and libraries reporting their drive serial number.
- You must correctly detect and configure every device to the operating system:
 - **Windows.** Devices should be available to the system Device Manager.
 - Library should be managed by the `Unknown Medium Changer` driver.
 - LTO drives should be managed by the `LTO` Windows native driver. See [LTO-7 Tape Drive](#) for details.
 - Other drives should be managed by the manufacturer's driver.
 - **Linux.** Devices should be listed by the `cat /proc/scsi/scsi` command. Tape drives should be managed by the `st` Linux native driver.

Device Connections

If your Host Bus Adapter (HBA) controller is optimized for RAID, then it is not compatible with tape drive and tape library use. The block size management of HBA controller is not adapted for sequential access devices (block size can be dynamically modified by the controller), nor for asynchronous data transfer.

Atempo is thus unable to support such a configuration for its products.

Libraries

These are the library prerequisites:

- Media Manager only supports libraries of these types:
 - SCSI/SAN/iSCSI/FC (Fiber Channel)
 - Other Library Managers (ACSLs)
- Media Manager only supports libraries providing barcode management capability:
 - Barcodes on media are mandatory. They must be reported by libraries, and they must be unique in the Miria configuration. Configure the library to report the full barcode to Miria, including the media ID suffix. See Administrator Documentation for details.
 - All barcodes used on media in libraries are supported, except the cleaning barcodes (i.e., barcodes that start with the CLN prefix). Cleaning barcodes must not be used on data media.
- Media Manager only supports tape libraries equipped with mailboxes.

ACSLs Libraries

To install a Media Manager server in an environment using ACSLS, request these items from your ACSLS administrator prior to the installation:

- A dedicated media pool.
- A dedicated barcode range.
- One or more dedicated tape drives.
- A CAP (Cartridge Access Port) in automatic mode.

If you use ACSLS, only one library can be declared on the ACSLS server and Media Manager only supports the standard port for ACSLS clients (i.e., `50004`).

Drives

Media Manager only supports drives connected inside a library (i.e., no drive management en standalone).

For an overview of drives supported by Miria, see the [Compatibility Guide](#).

Hardware Recommendations

- Avoid sharing a controller between disk and tape drives.
Atempo recommends that you dedicate a controller connection to disk(s) and another one to tape device(s).
- Use only generic controllers.
Do not use RAID-optimized controllers. Avoid using PowerEdge Raid Controller (PERC) and motherboard controllers because they are very likely to be optimized for RAID.

Device Configuration Limitations

- Media Manager does not support tape drives and tape libraries connected through NDMP.
- Media Manager does not support drive sharing with third-party software.
- Media Manager does not support library sharing with other applications (e.g., Atempo Tina), except with an ACSLS library.
Using the hardware split mechanism may alter and reduce the mailbox management functions.
- Media Manager does not manage or control the cleaning of tape drives.
Cleaning is managed by the library.
- When a SpectraLogic library is partitioned, the EE port must be configured in *shared* mode.
Media Manager does not support any other EE SpectraLogic modes.

Installation Parameters

Consider these recommendations:

- Selecting the Media Manager option automatically launches the Media Manager Setup on the current host.
- You can install the Media Manager server on any machine in the network.
The server implicitly includes an agent.
- You must install a Media Manager agent and a Miria agent on every machine physically connected to devices (i.e., libraries and drives).

The installation parameters are described in the table below.

For options to install Media Manager, see also [Installation Modes](#)

Parameter	Options and Actions
AMM Installation Type	<p>Choose whether you want to install a Media Manager server or agent.</p> <ul style="list-style-type: none"> Server installation. The Media Manager server is composed of the Media Manager database and a listener process communicating with the Media Manager agent(s). The Media Manager server is installed on the same machine as a Miria server or a Miria agent. You can install it on any platform with a compatible operating system. The Setup automatically installs the Media Manager server and database, and sets all the necessary environment variables. Agent installation. The Media Manager agent is composed of the services driving the libraries and/or drives. It must be installed on the platforms driving these devices. The Setup installs the library and media services, but not the database. The Setup sets all the necessary environment variables.
AMM Installation - Server Installation	<p>This screen displays only if the default ports are already in use.</p> <p>Media Manager uses these ports:</p> <ul style="list-style-type: none"> AMM Port Number. Port that enables the Media Manager server and agents to communicate. The default value is 651. <div> Note: The port must be open on the firewall from Media Manager agents to the Media Manager server. </div> Database Port Number (PostgreSQL). Port through which the Media Manager PostgreSQL database will listen. The default value is 15432. AMM HTTP Port Number. Port that enables Media Manager to communicate with Miria. The default value is 8282.
Media Manager - Agent Installation	<p>Complete these fields:</p> <ul style="list-style-type: none"> Server Name. Media Manager server with which this agent will communicate. Server Port. Port number that enables the Media Manager server to communicate with the agents. By default, the port is 651, but you can change it if necessary.

Parameter	Options and Actions
Device Detection	<p>Only for an agent installation. For a server installation, the automatic device detection is launched systematically.</p> <p>Once you have entered all installation parameters, the Installation Wizard proposes to run a storage device detection. The detection may reset existing devices and interrupt any running archiving jobs, and may take some time.</p> <ul style="list-style-type: none"> Click Yes to run the automatic device detection at the end of the installation. <p>Or</p> <ul style="list-style-type: none"> Choose No to manually launch the device detection later.

For more information on Media Manager, see the Administrator Documentation.

Device Configuration

Once the Miria Setup has successfully installed Media Manager, you are ready to configure devices in Media Manager, using one of these methods:

- Automated device configuration.** Configures the local SCSI devices with a serial number.

The Miria installer automatically launches the Automated device configuration when you install a Media Manager server from the Miria installer.

See [Device Configuration Prerequisites](#) before configuring your devices in automated mode.

Note: Atempo strongly recommends that you use automated device detection whenever possible. Automated detection makes it easier to keep the configuration consistent.

- Interactive device configuration.** Configures specific local SCSI devices or ACSLS.

Automated Device Configuration

Use the Automated Device Configuration feature if you want to configure all the local SCSI devices with a serial number.

The Miria installer launches the automated device detection when you install a Media Manager server from the Miria setup. When you install a Media Manager agent, the Miria installer asks you to choose if you want to run the automated device detection when the installation is complete. If you chose not to run automated detection, or if it ran but no local SCSI devices were detected (e.g., if they were not yet connected), then you must launch this procedure at your convenience after installing the product.

Recommendations

Review these considerations carefully before performing an automated configuration:

- Automated detection only applies to devices that are physically connected to a machine (i.e., SCSI, SAN, SAS, and Fiber Channel).
- Before performing any configuration using the `mm_adm_device` command, you must stop the `mm_agent` service.

See the Administrator Documentation.

See [Device Configuration Prerequisites](#) also before configuring your devices in automated mode.

SCSI Devices

Local SCSI devices are devices that are physically connected to a machine (Parallel SCSI, SAN, SAS, and Fiber Channel).

To create a local SCSI device in automated mode

1. Stop the `mm_agent` service.
2. Run Media Manager Command Line Interface.
3. Run `mm_adm_device` in automated mode:

```
mm_adm_device -a
```

All the local SCSI devices present on the agent are detected and automatically created in Media Manager.

Example.

```
...\bin>mm_adm_device -a
Creation of the drive with the serial number HU164604P2
Creation of the library with the serial number HU164604P6
Serial number HU164604P6 configured in C:\conf_drv\SN_HU164604P6.conf
configuration file
```

4. Start the `mm_agent` service.

Interactive Device Configuration

Use interactive device configuration if you want to configure specific local SCSI devices or ACSLS libraries.

Recommendations

Review these considerations carefully before performing an interactive configuration:

- Before you make any configuration change using the `mm_adm_device` command, you must stop the `mm_agent` service.

See the Administrator Documentation.

- You must declare all the drives that are connected to a library, even if you only want some of them to be used with Miria.

Otherwise, the library itself will not be correctly configured.

See [Device Configuration Prerequisites](#) before configuring your devices in interactive mode.

SCSI Devices

Local SCSI devices are devices physically connected to a machine (Parallel SCSI, SAN, SAS, and Fiber Channel).

To configure specific local SCSI devices, use the interactive mode.

To create a local SCSI device in interactive mode

1. Stop the `mm_agent` service.
2. Run Media Manager Command Line Interface.
3. Run `mm_adm_device` in interactive mode:

```
mm_adm_device
```

4. Scan the devices on the local host:

```
scan
```

5. If the serial number is available, create the new device with this command:

```
create <device_serial_number>
```

Or

You can use the scan list to create the new device (this is the only way for devices without a serial number):

```
create
```

6. Start the `mm_agent` service.

Example 1. Creating a device with a serial number.

```
(MM) scan
Device Type=Tape drive
Device Descriptor=c4b0t0l0
Configured=Yes
OS Device Path=\\.\Tape0
OS SPT Device Path=\\.\Tape0
Vendor Identification=HP
Product Identification=Ultrium 2-SCSI
Product Revision Level=kn77
Tape Drive Serial Number=HU164604P2
Number of <Product> drive type for this device=1
<Product> type value for this drive=44
=====
Serial number HU164604P6 already configured in C:\conf_drv\SN_
HU164604P6.conf configuration file
Device Type=Medium changer
Device Descriptor=spt_c4b0t1l0
Configured=Yes
OS Device Path=\\.\scsi4:
OS SPT Device Path=\\.\scsi4:
Vendor Identification=HP
Product Identification=1x8 G2 AUTOLDR
Product Revision Level=kn77
```

```

Library Serial Number=HU164604P6
Number of slots=8
Number of drives=1
Number of mailbox slots=1
Drives Serialization=Yes
Serial number for drive index0=HU164604P2
Number of <Product> library type for this device=1
<Product> type value for this library=240
Tina type name for this library=HP StorageWorks 1x8 G2
Split=No
=====
(MM) create HU164604P2
Creation of the drive with the serial number HU164604P2
(MM Create) Name of the device? HU164604P2

```

Example 2. Creating a device with or without a serial number (using the scan list).

```

(MM) create
Device Type=Tape drive
Device Descriptor=c4b0t0l0
Configured=Yes
OS Device Path=\\.\Tape0
OS SPT Device Path=\\.\Tape0
Vendor Identification=HP
Product Identification=Ultrium 2-SCSI
Product Revision Level=kn77
Tape Drive Serial Number=HU164604P2
Number of <Product> drive type for this device=1
<Product> type value for this drive=44
=====
(MM Create) Define this device on this host? (yes/no/cancel) yes
Creation of the drive with the serial number HU164604P2
(MM Create) Name of the device? mylib
Device Type=Medium changer
Device Descriptor=spt_c4b0t1l0
Configured=
OS Device Path=\\.\scsi4:
OS SPT Device Path=\\.\scsi4:
Vendor Identification=HP
Product Identification=1x8 G2 AUTOLDR
Product Revision Level=kn77
Library Serial Number=HU164604P6
Number of slots=8
Number of drives=1
Number of mailbox slots=1
Drives Serialization=Yes
Serial number for drive index0=HU164604P2
Number of <Product> library type for this device=1
<Product> type value for this library=240
<Product> type name for this library=HP StorageWorks 1x8 G2

```



```
Split=No
```

```
=====
(MM Create) Define this device on this host? (yes/no/cancel)
```

ACSL S

ACSL S is an Automated Cartridge System Library Software.

See [ACSL S Libraries](#) for more information on the prerequisites for creating an ACSL S library.

To create an ACSL S library

1. Stop the `mm_agent` service.
See the Administrator Documentation.
2. Run Media Manager Command Line Interface.
See the Administrator Documentation.
3. Run `mm_adm_device` in interactive mode:

```
mm_adm_device
```

4. Create an ACSL S library:

```
acslib
```

5. Provide this information:

- The ACSL S server name.
- The ACSL S library logical name.
- The ACSL S pool number.
- The range of barcode (optional).
- The drive type: Media Manager automatically detects whether the ACSL S server has several drive types and displays the “Select drive type for the current library:” message.

Select the drive type to declare because Media Manager can only manage one type of drive.

Note: If you do not specify neither the pool number nor the barcode range, Media Manager takes into account all the media of all the ACSL S pools, whatever their barcodes.

6. Start the `mm_agent` service.
See the Administrator Documentation.

Example.

```
(MM) acslib
(acslib) ACSL S server name? sonny
(acslib) ACSL S Library logical name? ACSL S_SONNY
(acslib) ACSL S pool [*]? 124
(acslib) Range of barcode [*]? 000000-999999
```



CHAPTER 5 - Updating Miria

This topic describes how to update Miria.

Update Checklist

This table describes the recommendations that you must take into account before running an update of a Miria installation:

Environment	Recommendations
General	<p>Take into account these recommendations:</p> <ul style="list-style-type: none">• Before you update the Miria server, Atempo recommends that you back up your Miria database. For more information on database backup, see the Administrator Documentation.• When upgrading from a version < 3.10, you must migrate the internal ADA database & AMM database to the latest version. See also Migrating the Database from a Version prior to 3.10• All the Miria installation components must be of the same version. If you update one component (e.g., the server), you must also update all the agents, interfaces, optional modules, etc., from the same distribution.
Media Manager	<p>Close any Media Manager Command Line utilities before you run the update.</p>

Update Types

You can perform the following types of updates:

- **Typical.** Updates all your existing components and options to a more recent version, but you cannot add options.
- **Custom.** Updates your existing components to a more recent version, but it also enables you to install other components such as Media Manager.

Updating in Graphical Mode

1. Follow the same procedure as for installation.
If the Installation wizard detects an environment on the system, it passes automatically into Update mode.
2. Follow on-screen instructions, as for installation, with these differences:

- If the Installation wizard detects that the Content Indexing option is installed in your environment, it displays a warning and stops the installation. Click Quit installation on the warning window and uninstall the Content Indexing option as described in [Uninstalling Miria](#). Then, resume the update.
- In Custom mode, an Optional Components window enables you to add or remove the options. By default, options already installed are updated. If you want to install additional options, select the corresponding check boxes.

Updating Components from the CLI

Components can be updated interactively or in silent mode from the command line interface. See also [Installation Modes](#)

- > Follow the same procedure as for the installation. Update mode is automatically activated when an environment on the system is detected.

CHAPTER 6 - Uninstalling Miria

This topic describes how to uninstall Miria components. Uninstalling the Miria server or agent uninstalls Media Manager as well.

1. Launch the Uninstall Wizard in the manner corresponding to your operating system.

Tip: For Linux and Windows only: By default, the same uninstallation mode is used as for the installation. To select another uninstallation mode, you can use the `./Uninstall -i gui` command.

This table describes the actions that you can perform in the Uninstall Wizard depending on your operating system:

Operating System	Uninstall Actions
Windows	<p>Perform these actions:</p> <ol style="list-style-type: none">1 Run Control Panel > Programs (or Add or Remove Programs on earlier Windows versions).2 Select Miria in the Programs and Features window.3 Run Uninstall. <p>The uninstallation automatically uninstalls the PostgreSQL or MaxDB component. Do not uninstall PostgreSQL or MaxDB manually if you want to run a complete clean uninstall.</p>
macOS	<p>Perform these actions:</p> <p>Open a Terminal as root and launch <code>/Applications/Miria/Uninstall/uninstall_all.sh</code>.</p> <p>Note: Do not select a sub-program such as <code>Uninstall_Miria</code>, <code>Uninstall_ADARuntime</code>, etc., if you want to run a complete clean uninstall.</p>
Linux	<p>Perform this action:</p> <p><code>cd</code> to the directory where Miria was installed (e.g., <code>/root/Miria</code>) and run the <code>./Uninstall/Uninstall</code> program at the command line prompt.</p> <p>Note: Do not select a sub-program such as <code>Uninstall_Miria</code> or <code>Uninstall_ADARuntime</code> if you want to run a complete clean uninstall.</p>

2. Follow on-screen instructions in the **Uninstall Wizard**.
3. In the **Uninstall Options** window, select one of these options:
 - **Complete Uninstall**. This is the recommended option.
 - **Partial Uninstall (Keep Miria's database)**.
4. Click **Uninstall**.

CHAPTER 7 - Use Case #1 - Archiving Data from NAS

This topic provides a step-by-step guide for configuring Miria to archive data from network attached storage (NAS) to disk, and then retrieve it from archived storage.

If you have not yet installed Miria, see [Installing Miria Server](#).

See also Administrator Documentation, as well as the documentation for your NAS.

System Requirements

Before you begin this procedure, ensure that both your NAS and Miria meet these initial requirements.

CIFS/SMB NAS

The CIFS/SMB NAS requires a shared directory from which you want to archive data. The shared directory must exist before you configure Miria, and it must be accessible by a UNC path. For example: \\ServerName\Share. Do not use a drive mapping, because the mapping is associated with a specific user and will not be accessible by Miria. When you configure Miria for archiving, you will specify the name of a user who has full permission to that share.

Miria

These are the Miria requirements:

- License to install and use Miria.
- Miria Server installed on any supported operating system. This guide uses a Windows server installation as an example.
- Miria Agent on the server with full permission to the NAS from which you want to archive data.
- Administration Console installed on a workstation or server with a connection to Miria Server.
- At least one user with full permission to Miria Server. This user is called the Super User; in this procedure, the user is *root*. For more information on working with users, see the Administrator Documentation.

Naming

In this topic, these names will be used in the examples to identify the required Miria objects.

To simplify your configuration, you can substitute your own names and note them in this table:

Object	Example Name	Your Name
Source Agent (Archiving Platform)	dell-sc440	
Source data location	\\dell-sc440\c\MiriaSource	
Destination Agent (Archiving Platform)	Dell-T110	
NAS Archiving Platform	NAS2	
Storage Manager	SM on T110	
Storage Manager Container	SMC on T110 C:\MiriaDest	
Retention Period	Year	
Archiving Policy	My NAS Archiving Policy	
Project Archive	NAS Project Archive	
Task	ArchiveNASProject	

Data Flow Diagram

This diagram shows the component configuration when you configure Miria to archive data from NAS to disk on a file server ([Figure 3](#)).

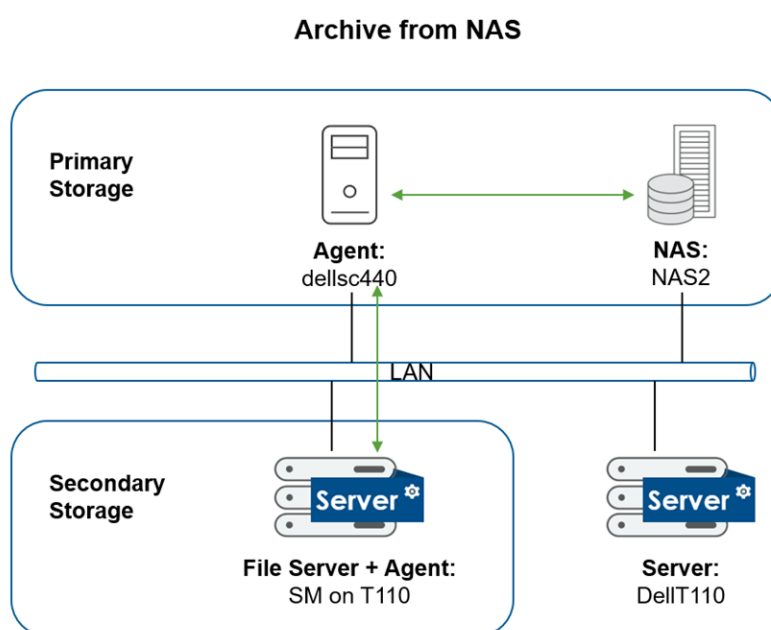


Figure 3: Archiving data from NAS to disk on a file server

Configuring Miria to Archive from NAS

Any time you configure archiving, you must specify the archiving source, which is the primary storage from which data will be archived, and the archiving destination, which is the secondary storage where it will be stored. You must also configure archiving policies to determine where data will be archived and how long it will be retained.

Process Overview

In Miria, this process includes these steps:

1. **Connecting to the Administration Console.**
When you first log on to the Administration Console, you must specify the Miria server and database instance that you want to reach.
2. **Configuring the Archiving Source.**
The first step in archiving configuration is to identify the source from which you want to archive files. In this procedure, you specify the NAS as the source of archive data, or the primary storage. Since you cannot install a Miria agent on NAS, you must install it on a machine with access to the NAS. The Miria Agent on that machine then archives the data from the NAS by proxy. In this configuration, you must first identify the agent machine as the Archiving Platform in charge of data movement for the NAS. You then must declare the NAS from which the agent is archiving data as a second Archiving Platform.
3. **Configuring the Archiving Destination.**
After you have configured the source of archiving, you must configure the archiving destination—the secondary storage server on which archived data will be stored. First you must identify that destination as another Archiving Platform to which a Miria Agent will be writing data. Then define the archiving destination by both the Storage Manager, which is the server on which data will be stored, and the Storage Manager Container, which is a named location on the Storage Manager.
4. **Creating the Retention Period.**
The retention period determines how long archived data will be saved.
5. **Creating the Archiving Policy.**
The archiving policy associates the storage manager container, where archived data will be stored, with a retention policy. The result is an archiving policy that determines how long data will be retained on a given storage manager container.
6. **Creating the Project Archive.**
The project archive grants one or more users permission to archive and retrieve data.

The remainder of this section provides step-by-step instructions for completing each of these procedures.

Note: Miria provides smart defaults for many advanced configuration parameters. The procedures in this section use these defaults and describe only minor changes required. To learn more about the advanced settings available, see the Administrator Documentation.

Connecting to the Administration Console

In this procedure, you launch Administration Console for the first time by specifying the Miria server name to which you want to connect.

This documentation uses a Windows installation as an example.

To log in to the Administration Console

1. Select Start › Programs › Miria › Miria Administration Interface.
The Login window opens.
2. Enter these parameters:
 - **User.** Enter `root`.
 - **Password.** Leave this field blank.
 - **Connect in Super User Mode.** Select this box.
 - **Miria Server.** Enter the Miria server machine name.
If you modified the default port for Apache http connection (`80`) during Miria custom installation, add this custom port to the server name.
The format is:
`server_name:port_number`
For instance, if you chose port `85` instead of `80`, and the server name is `adadoc`, enter `adadoc:85` in the Miria Server field.
 - **Database Name.** Choose the database instance, by default, `Miria`.
 - **Proxy I/O Domain.** Leave this field empty.
 - **Debug.** Leave this option set to None.
3. Click Login.

The next time you launch the Administration Console, you will be automatically connected to the server and database instance that you specified here.

Configuring the Archiving Source

In this procedure, you configure Miria to archive from network attached storage to disk. Since you cannot install Miria Agent directly on an NAS device, you must install Miria Agent on a server that has direct access to NAS.

You will declare the combination of the Miria system that will perform the archiving tasks and the NAS from which data is archived as the Archiving Platform, thereby enabling Miria to recognize the location as an archiving source.

This procedure includes two steps:

- Declare the source archiving agent.
- Configure the NAS as the source of the archive data.

To declare the source archiving agent

1. Open the Administration Console (Figure 4).

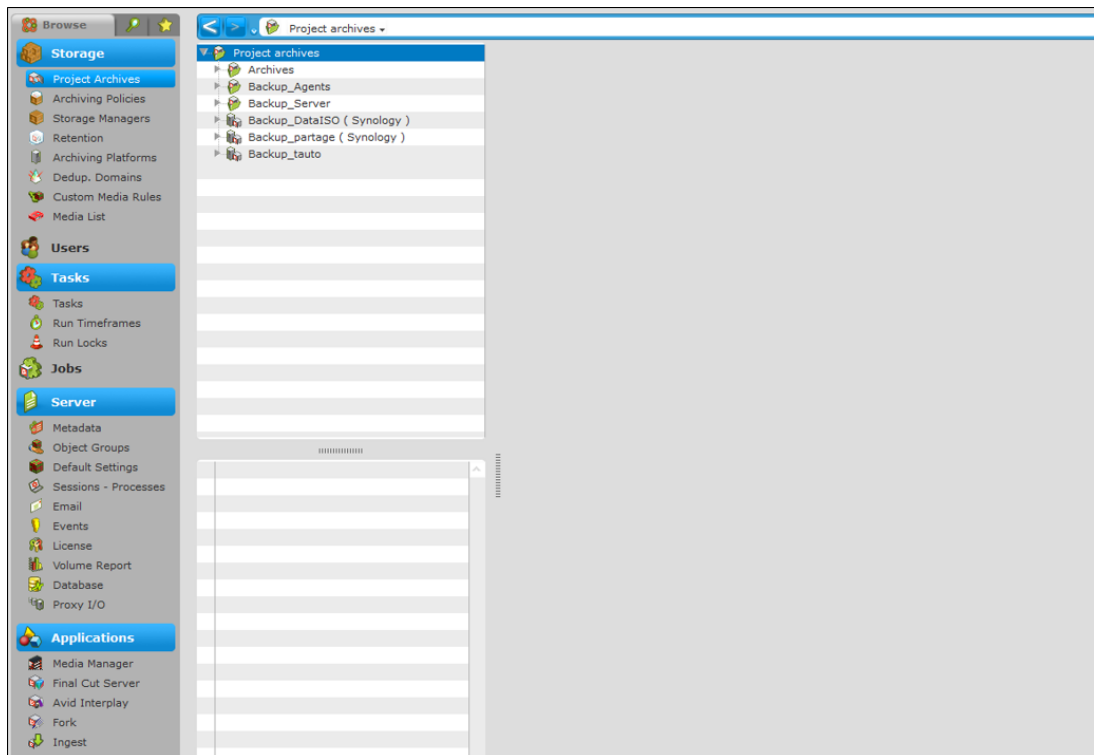


Figure 4: Administration Console interface

2. On the left pane, select **Storage > Archiving Platforms**.
3. On the confirmation message that opens, click **Yes**.

Note: If you have already set up at least one archiving platform, then the Archiving Platforms page opens in the right pane. Click **New [+] > New Archiving Platform**.

The Platform Configuration window opens (Figure 5).

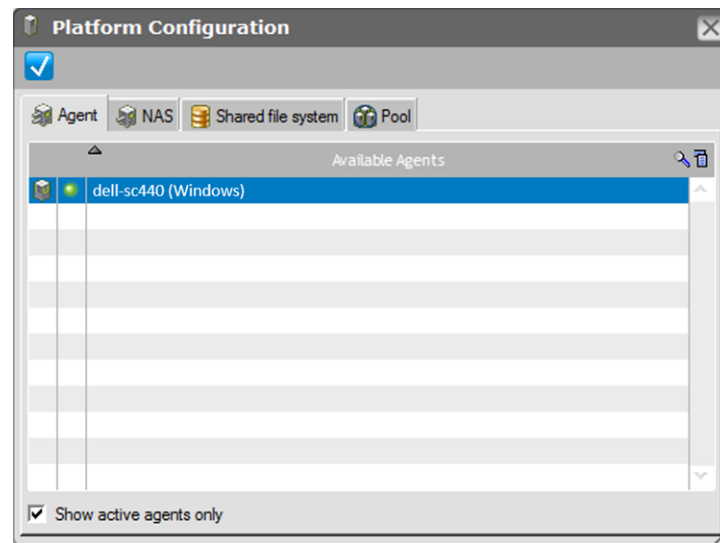


Figure 5: Source archiving agent configuration

4. Choose the agent located on the server with direct access to the NAS share that contains the source data.

In this example, the source system is dell-sc440.

5. To accept these changes, click ☒ in the upper left corner.

The **Platform Properties** pane is displayed (Figure 6)

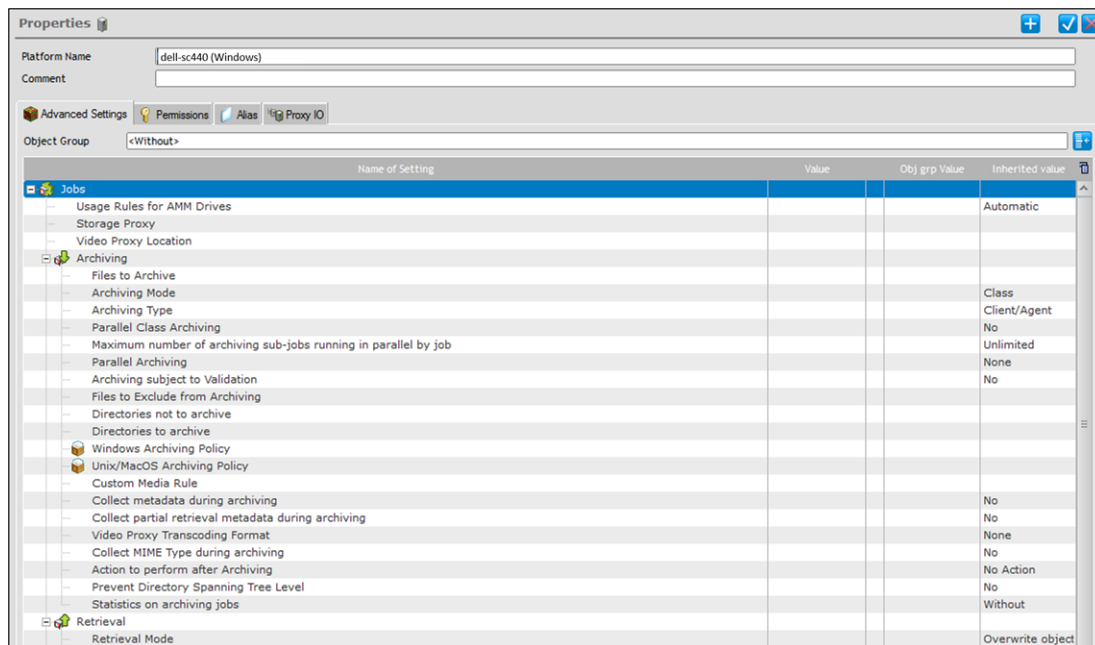


Figure 6: Source archiving agent properties

6. Keep the default configuration parameters specified in the Advanced Settings table.
7. Click ☒.

To configure NAS as the source of archive data

1. On the left pane, select **Storage > Archiving Platforms**.
2. Click New [+] > **New Archiving Platform**.
3. Select the **NAS** tab.
4. In the **Platform Name** box, type a name for the NAS archiving platform you are creating. Use a descriptive name, as you will specify this archiving platform again later in this configuration procedure. In this example, the Platform Name is **NAS2**.
5. From the NAS Type drop-down list, choose **Other** (Figure 7).

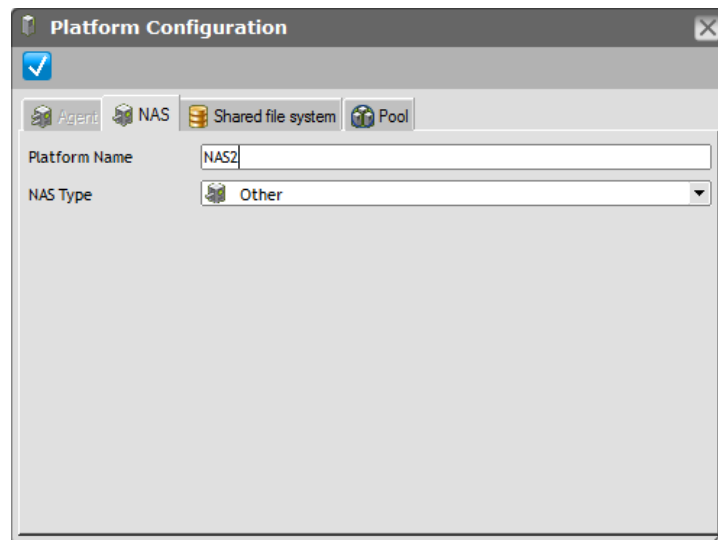


Figure 7: NAS archiving platform configuration

6. Click . The Properties pane is displayed (Figure 8).

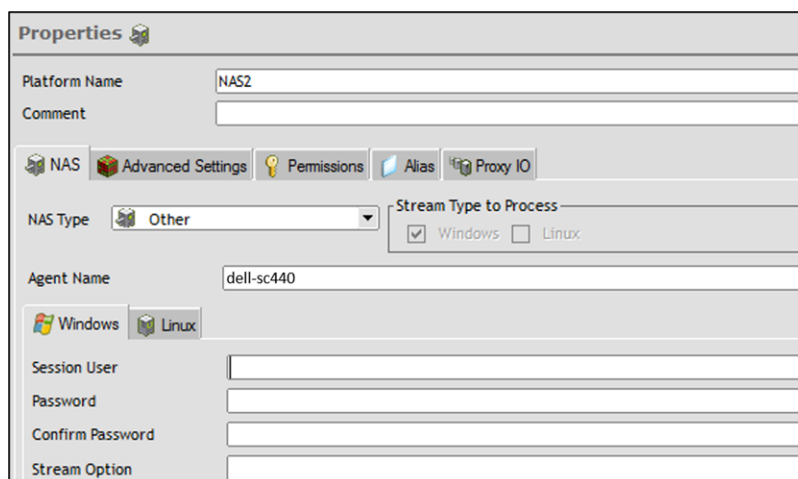


Figure 8: Archiving Platform properties

7. Under Stream Type to Process, select the check box beside the network protocol Miria Agent used to connect to the NAS.
Note that Miria will enable you to choose only the stream type that is supported by the agent. In this example, a Miria agent installed on a Windows server will be in charge of data

movement from the NAS, so select Windows (CIFS). If the agent was installed on Linux or macOS, you would choose Linux/macOS (NFS).

8. On the NAS Properties page, specify this information:
 - **Miria Agent.** Select the agent that you specified in the [To declare the source archiving agent](#) procedure. In this example, the Miria Agent is `dell-sc440`.
 - **Session User.** Type the name of a user who has Administrative permissions for the NAS. If the user you choose does not have administrative permissions, archiving will fail.
 - **Password.** Type the password for the specified user.
 - **Confirm Password.** Retype the password for the specific user.
 - **Stream Option.** Leave this option blank.
9. Click ☒.

Configuring the Archiving Destination

After you configure the source as an archiving platform, you must then create the storage area on the secondary storage device, which acts as the archiving destination.

Declaring the Destination Location as an Archiving Platform

In this scenario, you are archiving from NAS to disk, and the disk is on the Miria Server machine. You therefore must declare the Miria Server as the Archiving Platform of the secondary storage.

To declare the destination archiving agent

1. On the left pane, select **Storage > Archiving Platforms**.
2. On the **Archiving Platforms Properties** page, click New [+] > **New Archiving Platform**. The **Platform Configuration** window opens ([Figure 9](#)).

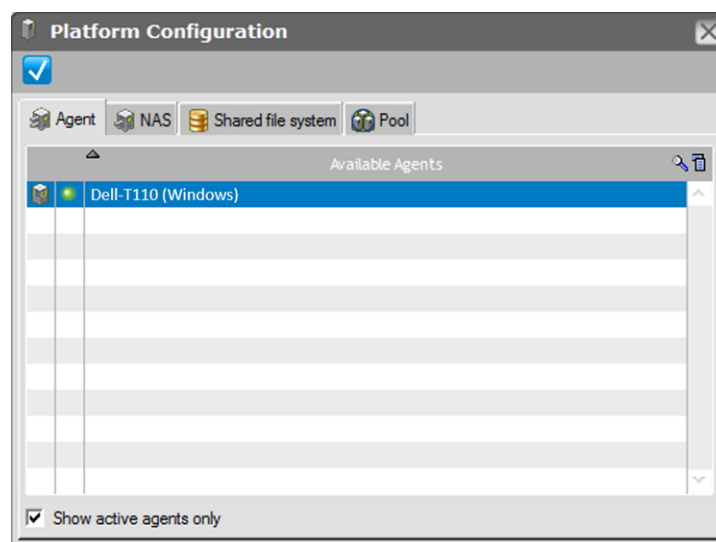


Figure 9: Destination archiving agent configuration

3. From the **Available Agents** list, choose the agent that will manage the archive destination. In this procedure, the agent is `Dell-T110`.
4. To accept these changes, click ☒ in the upper left corner.

The **Platform Configuration** dialog box closes, and the **Platform Properties** pane opens (Figure 10):

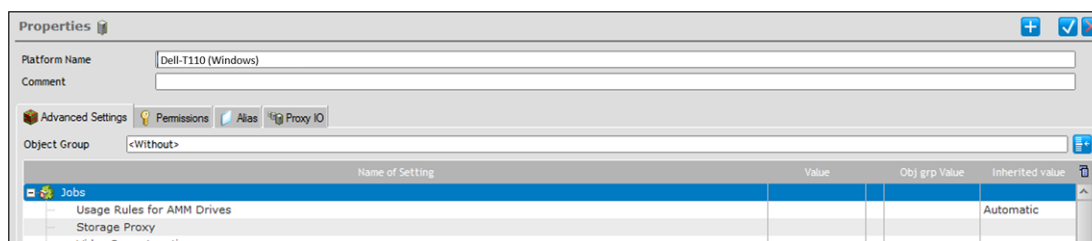



Figure 10: Destination archiving agent properties


5. Keep the default configuration parameters specified in the **Advanced Settings** table.
6. Click .

Configuring the Server and Shared Folder as the secondary storage

In this procedure, you define the Miria server as the Storage Manager (the archiving destination) and a Storage Manager Container (the directory on the archive destination) as follows.

To create the Storage Manager

1. On the Administration Console, under **Storage**, click **Storage Managers**.
On the confirmation message that opens, click **Yes**.

Note: If you have already set up at least one Storage Manager, then the Storage Managers page opens in the left pane. Click New  **New Storage Manager**.

The **Storage Manager Properties** window opens.

2. In the **Storage Manager Name** box, type a name for the Storage Manager you are creating. Use a descriptive name that you can reference easily in the remaining archive configuration. In this procedure, the name is **SM on T110**.
3. From the Type list, keep **File Storage One to One**. This option organizes archived data in a tree structure that mirrors the data on the source file system. One directory/file on the source file system corresponds to the same directory/file on the destination file system.
4. To ensure archiving will be active, in the Status drop-down, leave the default option (i.e., Online).
5. On the Configuration page under Miria File Storage One to One, click the **Select** button beside the **Storage Platform** box.

The **Platform List** opens (Figure 11).

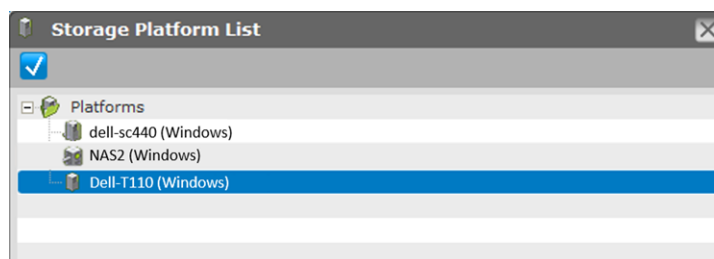


Figure 11: Destination archiving platform list

6. From the **Platform List**, click the archiving platform you created as the destination; in this procedure Dell-T110. Click ☒.
 7. On the storage manager Properties page, click ☒.
- The storage manager you created opens in the **Storage Manager list**.
You can now create the **Storage Manager Container**, which specifies the folder location where archived files will be stored.

To create the Storage Manager Container

1. On the Administration Console, under **Storage**, click **Storage Managers**.
The **Storage Manager** window opens.
2. On the **Navigation** pane, right-click the newly-created **Storage Manager**, and then select **New Storage Manager Container** (Figure 12).

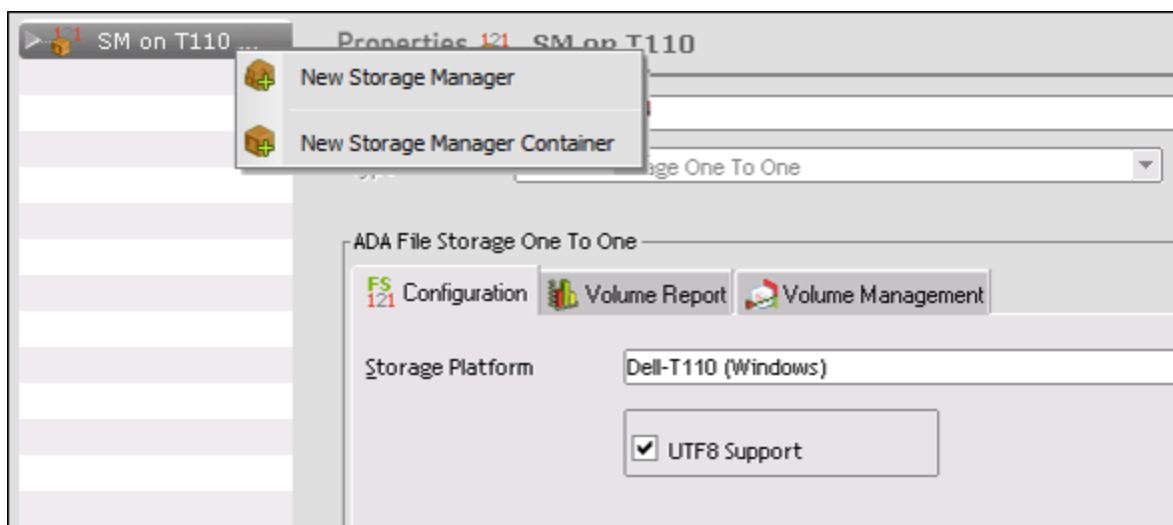


Figure 12: Create a new storage manager container

The Storage Manager Container Properties pane opens (Figure 13).

Figure 13: Storage manager container properties

3. In the **Storage Manager Container Name** box, type a name for the container. Use a descriptive name that you can reference easily in the remaining archive configuration. In this procedure, the name is `SMC on T110`.
4. The **Storage Manager** box displays the name of the selected Storage Manager. You cannot edit this name.
5. Leave the **Deduplication Domain** blank.
6. From the **Run Lock** list, choose <without>.
7. Under Miria **File Storage One to One**, the Master Storage Platform displays the name of the archiving platform that you created earlier and associated with the storage manager. You cannot edit this name.
8. In the **Directory** box, type the absolute path to the directory where you want to archive your data on the storage manager. You must create this folder on the file system and ensure that it is shared and accessible before configuring Miria to recognize it as a storage manager container. In this procedure, the path is `C:\MiriaDest`.
9. From the **Digest on Storage** list, choose **None**.
10. From the **Data Compression** list, choose **None**.
11. Click

Creating the Retention Period

After you have configured both the NAS archiving source as an archiving platform, and the destination storage manager container, you must define a retention period. The retention period defines the period of time that the archived data will be saved on your storage manager before it is deleted.

To create the retention period

1. On the Administration Console, under **Storage**, click **Retention**.
2. On the confirmation message that opens, click **Yes**.

Note: If you have already set up at least one Retention Period, then the Retention Period Properties page opens in the right pane. Click New [+] > **New Retention**.

The Retention Properties pane opens (Figure 14).

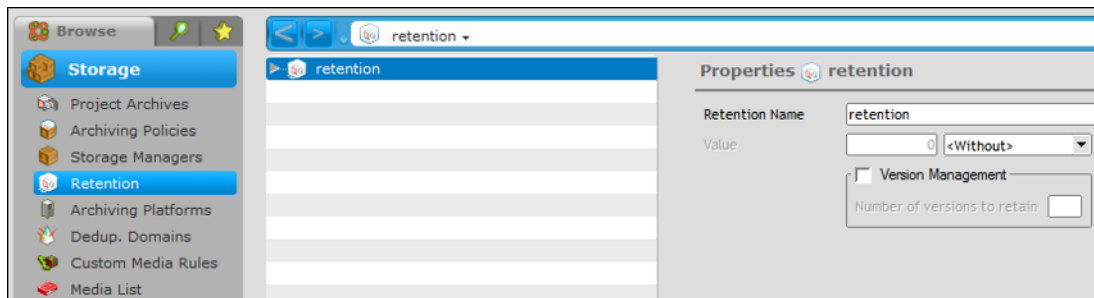


Figure 14: Retention properties

3. In the Retention Name box, type a name for the retention period. Again, use a descriptive name, as you will specify this retention period in subsequent configuration steps.
In this procedure, you are configuring Miria to retain data for one year, so the name is **Year**.

Note: By default, data is retained permanently—it is never deleted. This configuration is represented by a blank Value and <Without> selected in the drop-down list.

4. To define a specific retention period, choose a unit of time from the drop-down list: Days, Weeks, Months, or Years, and then type the number of that unit you want to retain the data into the Value box.
For this example, choose Years from the drop down list, and then type **1** into the Value box.
5. Click ☒.

Creating the Archiving Policy

Now that you have created both a storage manager container for housing the archived files, and a retention period to dictate how long archived files are saved, you can create an archiving policy. The archiving policy associates a storage manager container with a retention period, thereby defining how long archived data is retained on a particular system.

To create the archiving policy

1. On the Administration Console, under Storage, click **Archiving Policies**.
2. On the confirmation message that opens, click **Yes**.

Note: If you have already set up at least one archiving policy, the archiving policy Properties page opens in the right pane. Click New [+] > **New Archiving Policy**.

3. In the **Archiving Policy Name** box, type a name for the policy. In this procedure, the name is **My NAS Archiving Policy**.

4. In the **Comment** box, type a description of this archiving policy (e.g., Archive on T110 and retain for a year).
5. Beside the **Retention Name** box, click the **Select** button.
The **List of Retention Periods** window opens (Figure 15).

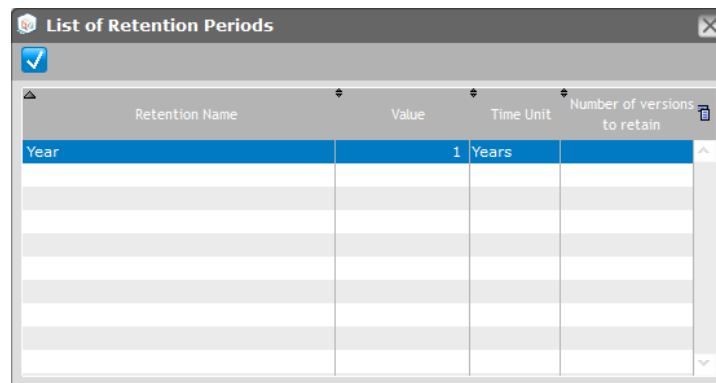



Figure 15: List of retention periods

6. Click the **Retention Period** you created in the previous procedure (i.e., Year) and then click .
7. Beside the **Storage Manager Container List**, click the **[+]** button.
The **List of Storage Manager Containers** window opens (Figure 16).

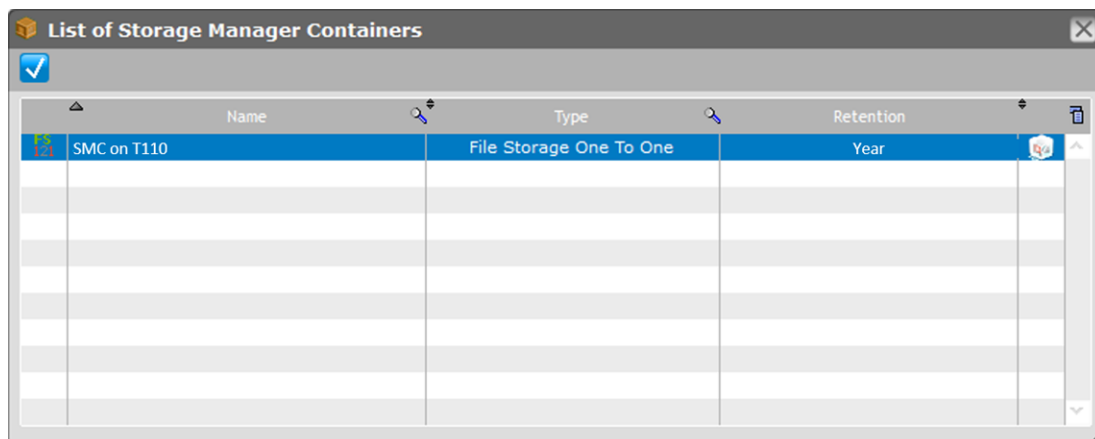




Figure 16: Storage manager container list

8. Select the name of the storage manager container that you want to associate with the selected retention period to create an archiving policy (in this procedure SMC on T110), and then click .

- On the archiving policy Properties pane, click . The policy is created (Figure 17).

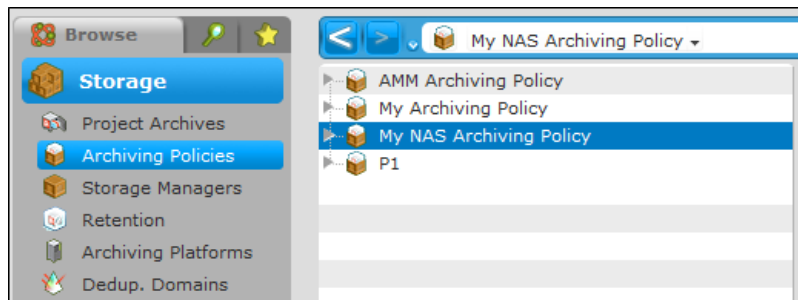


Figure 17: Archiving policy

Creating the Project Archive

The final step in the storage configuration process is to create the Project Archive. The project archive represents the container in Miria through which you can access archived data using the Administration or User Interface. You will also use the project archive to set up a task to archive data.

To create the project archive

- On the Administration Console, under **Storage**, click **Project Archives**.
- Right-click the **Project Archives** list in the center pane, and then click **New Project Archive** (Figure 18).

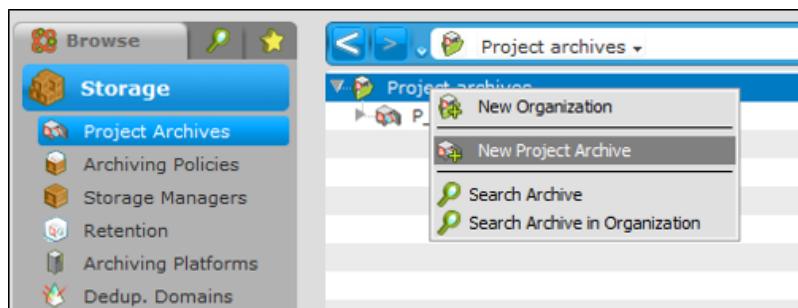


Figure 18: New project archive selection

- In the **Project Archive Name** box, type a name for this project archive. In this procedure, the name is `NAS Project Archive`.

4. Beside the Owner box, click the **Select** button. The list of users is displayed (Figure 19).

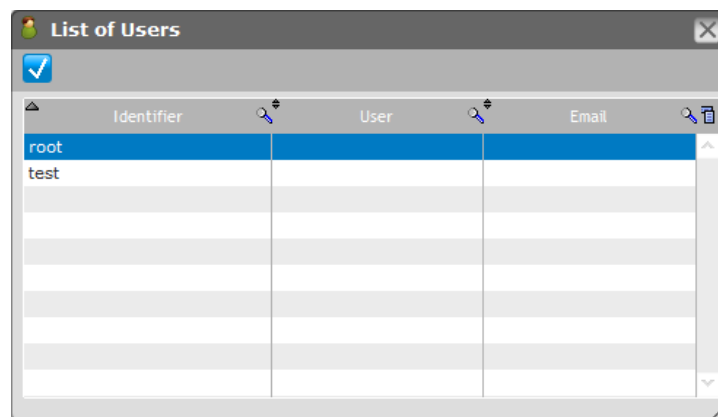


Figure 19: List of users

Select the **root** user, and then click the check mark.

5. Click the **Permissions** tab. Initially, both lists on the Permissions page are disabled.
6. To enable the controls, you must add a user to whom you want to grant permissions. Click the [+] to add a user. The Selection of Users and Overall/LDAP groups list opens (Figure 20).

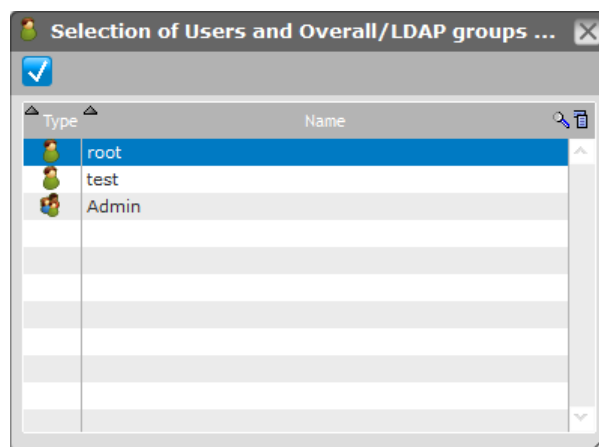


Figure 20: User and user group selection

7. From this list, select **root**, and then click ☒.
8. With **root** selected in the User or Group Name list, select the Allow check box at the top of the Permissions table to grant all rights to **root** (Figure 21).

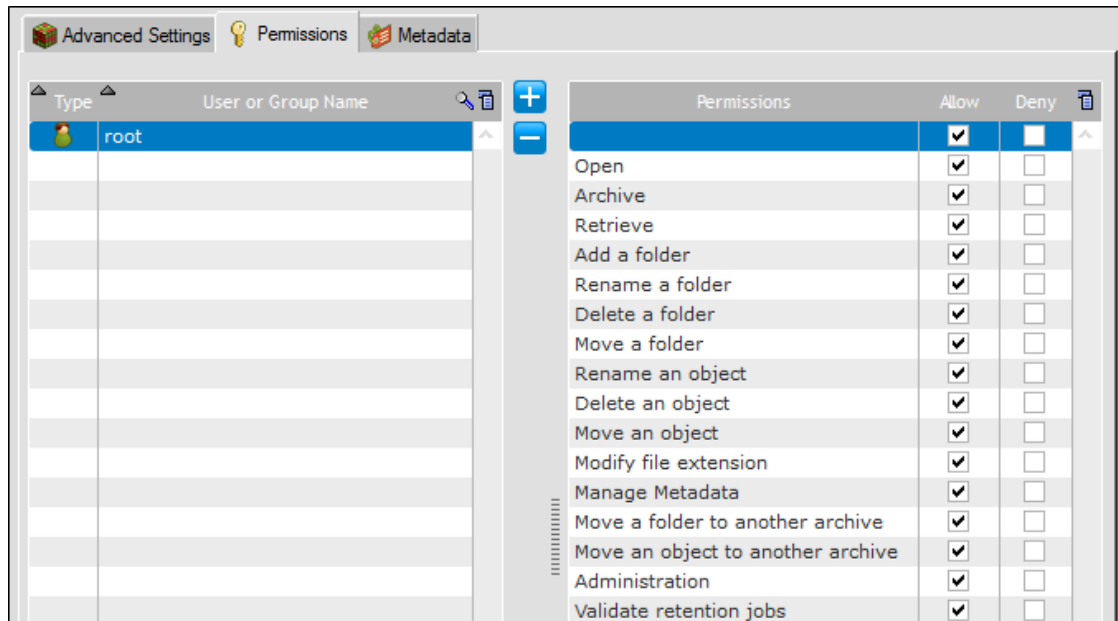


Figure 21: All rights are granted to `root`

9. Click .

Creating an Archiving Task

In this procedure, you will perform archiving using a named task in Miria. This configuration uses the parameters that you configured in the [Configuring ADA to Archive from NAS](#) section to create a specific task from which you can launch and monitor the archiving job.

This procedure is an example of the many options that you have for configuring Miria.

Creating the Archiving Task

In this procedure, you create an archiving task to archive data from your preconfigured archiving platform (source) to the storage manager container (destination) based on the Automatic Archiving task template. You can select a particular path on the source archiving platform to archive, and choose a destination name for the archived data.

You set a schedule to run the task automatically at specific times. Once the task is configured, you perform an initial manual run. Although you run the task manually as part of these instructions, automatic scheduled runs are the typical configuration.

To create an archiving task

1. On the Administration Console, select **Tasks > Tasks**.
2. To create a new task, on the **Task Properties** window, click **[+] > New Task**.
3. From the **Template list**, select **Automatic Archiving** ([Figure 22](#)). This enables the Configuration page of Task Properties for editing, and populates the remaining advanced settings with smart defaults for your archiving task.

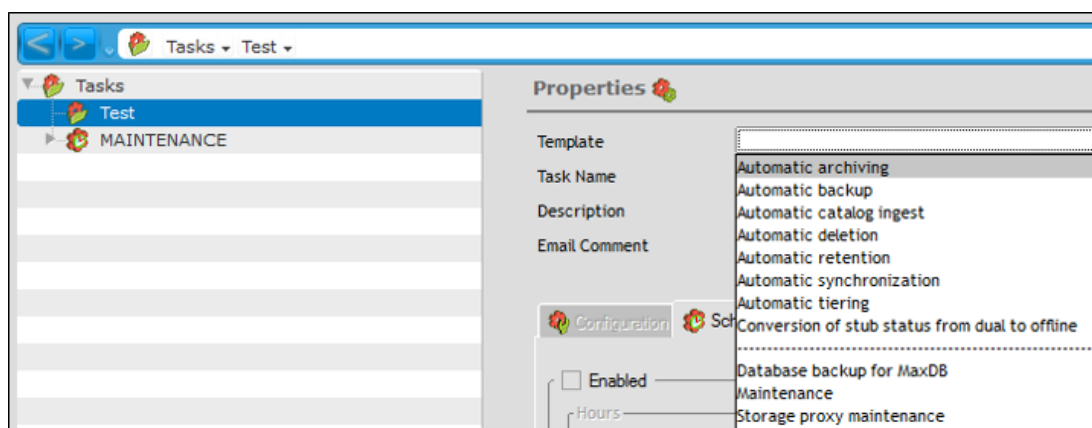


Figure 22: Automatic archiving template for a new task

4. In the **Task Name** box, type a name to identify this task within Miria.
Note that the name must not contain spaces.
In this procedure, the name is `ArchiveNASProject`.
 5. In the **Description** box, type a detailed description of the task, such as `Archiving task to my NAS project archive`.
 6. For now, you can leave the **Email Comment** box blank.
- Note:** You can use this option to specify any text you want to e-mail to authorized users when the task is triggered; however, to complete this configuration, you must also set up an SMTP server within Miria.
7. Ensure that the **Configuration** tab is selected.
 8. Configure the Source by specifying these parameters:
 - From the Storage Platform list, choose the archiving platform you created for the NAS in [Configuring the Archiving Source](#). In this example, it is `NAS2`.
 - In the Loc of Data to Archive box, type the root of the path from where archiving should start (e.g., `C:\MiriaSource`). This folder and all subfolders of the specified path will be archived.
 9. Under **Destination**, keep the default Archive Name (i.e., Full Path Auto-generated) and then click the select button to the right of the edit box.
 10. Choose a project archive, which in this procedure was named `NAS Project Archive`, and then click ☒. When archiving begins, Miria create a mirror of the source path within the storage manager container.
 11. Choose your archiving policy ([Figure 23](#)):
 - a. Click the **Advanced Settings** tab.
 - b. Under **Jobs**, click the box in the **Value** column beside Windows Archiving Policy (or Linux/macOS Archiving Policy if that is your destination operating system).
 - c. From the drop-down that opens, choose the archiving policy you created. In this procedure, the name is `My NAS Archiving Policy`.

Properties

Template: Automatic Archiving

Task Name: ArchiveNASProject

Description: Archiving task to my NAS project archive

Email Comment:

☐ Task not active

Configuration Scheduling Email Advanced Advanced Settings

Object Group: <Without>

	Name of Setting	Value	Ob
[-] Jobs			
	Action to perform after Archiving		
	Windows Archiving Policy	My NAS Archivin	

Figure 23: Archiving policy selection

12. Configure an automatic task schedule:
 - a. Click the Scheduling tab.
 - b. Select the Enabled check box.
 - c. Select the check boxes beside the Hours, Days, and Occurrences when you want to run the task. For example, to run the task the Last Friday of every month at 12:00 A.M., select:
 - Hours: 12 AM
 - Minutes: 00
 - Days: Friday
 - Occurrences in the Month: Last
 - Offset: No Offset
13. Keep all other defaults, and then click .
14. On the confirmation message, You have not defined any constraints. Do you want to validate anyway? click **Yes**.
 This **Task** will run automatically the last Friday of next month at 12:00; however you can test it and launch it manually beforehand to ensure that it runs properly.

Testing the Archiving Task

You can test the newly-created task before performing any actual archiving. This test verifies that Miria Agent has access to the source platform and is able to select the files to archive.

To test the archiving task

1. In the center pane, ensure that your new task is selected.

- Click on the microphone button to test the Task (Figure 24).

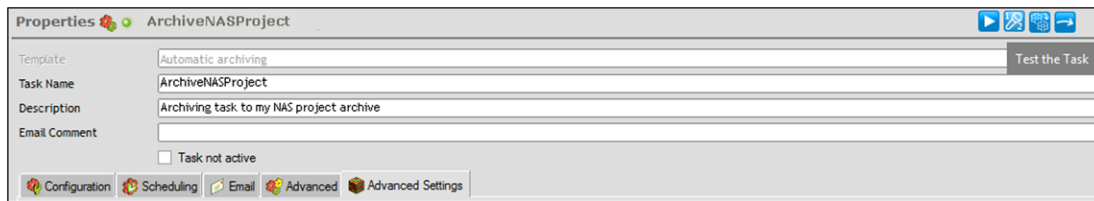


Figure 24: The microphone button is placed in the upper right corner

- On the confirmation message that opens, click **Yes**. Miria tests the parameters of the archiving task.
- On the confirmation message that opens, click **OK**. To validate the files and folders that will be archived as part of the task, you can review the **Event list**.
- In the left pane of the Administration Console, select **Server > Events**. This list displays all the files and folders that will be archived as a result of the archiving task. If the selection is not appropriate, you can edit the Task and configure constraints.

Archiving and Retrieving Data

After you have set up all of your archiving policies, and you have configured a task to perform the archiving job, you can archive and retrieve data.

In the following procedures, you archive data using the Miria Administration Console. You can also archive and retrieve data directly from the archiving source using the Miria User Interface.

Archiving Data

Based on the task schedule you set, data will be archived automatically on the last Friday of the next month. To manually archive data from the Administration Console, run the archiving task that you configured in the previous procedure.

To run the archiving task

- On the Administration Console, under **Tasks**, click **Tasks**.
- On the center pane, in the **Tasks list**, click the task that you created in the previous procedure.
- On right side of the **Tasks Properties**, click the **Run the Task** button (Figure 25).

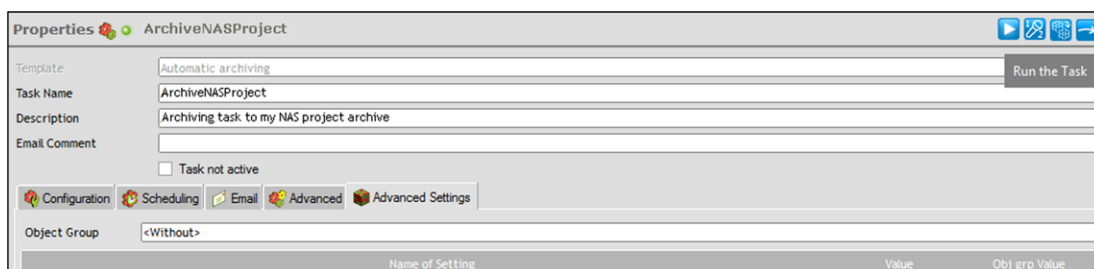


Figure 25: The Play button enables to run a task

- On the confirmation message that opens, click **Yes**.
Miria creates the archiving job, which will run in queue as soon as resources are available. On the confirmation message that opens, click OK.
- To monitor the **Archiving Job**, on the left pane of the Administration Console, click **Jobs**. The **List of Jobs** window is displayed (Figure 26).
- In the Current table, look for a job with the Action named Task.
Initially, the Job Status is In queue. Once the job begins to run, the status updates to Running. Finally, when the job completes, it is moved to the History table with a Job Status of Completed.

[illegible]

Figure 26: List of jobs and their corresponding status

7. Check the destination directory on disk to validate that the files have been archived successfully.
You can also verify in the project archive.

Retrieving a File

You can use the Administration Console to retrieve archived data. To do so, you must open the Project Archive, which contains a list of all archived data. From there, you can choose the data you want to retrieve.

If you are running Administration Console on a computer that does not have a Miria agent installed, then you must configure a Storage Proxy to complete the Retrieval. Under **Project Archives > Advanced Settings > Jobs > Storage Proxy**, locate the Value list drop-down menu and choose an existing Storage Manager Container of Miria File Storage One to One type, which will be used as a cache during the retrieval. If you do not have an available Miria File

Storage One to One Storage Manager Container, you can create one wherever you have adequate free space. See the Administrator Documentation.

To retrieve a file

1. On the Administration Console, under Storage, click Project Archives.
2. In the list in the center pane, right-click the Project Archive you created, and then choose Open Archive.

The Project Archive window opens and displays the contents of the archive ([Figure 27](#)).

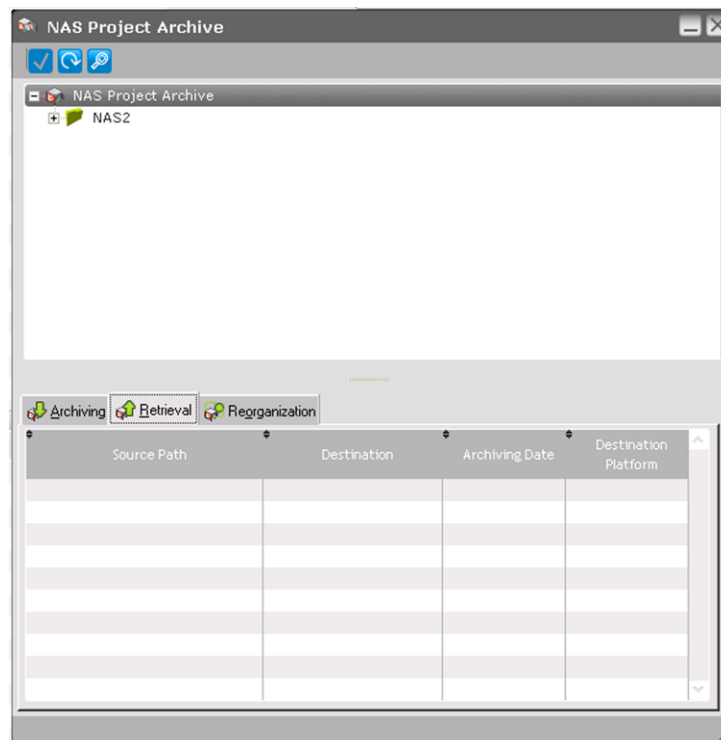


Figure 27: Archive contents

3. Expand the tree to navigate to the files that you want to retrieve.
4. To retrieve a file, right-click the file name in the tree and then choose Retrieve.
5. (Optional) In the Retrieval Destination dialog box, indicate the path of the file to retrieve in the Source field.
6. To the right of the Destination field, click on the Browse button. The Browse for Folder window opens.
7. On the local machine on which Administration Console runs, choose the path to save the retrieved data.
8. Click OK. The files you chose open in the Retrieval table ([Figure 28](#)).

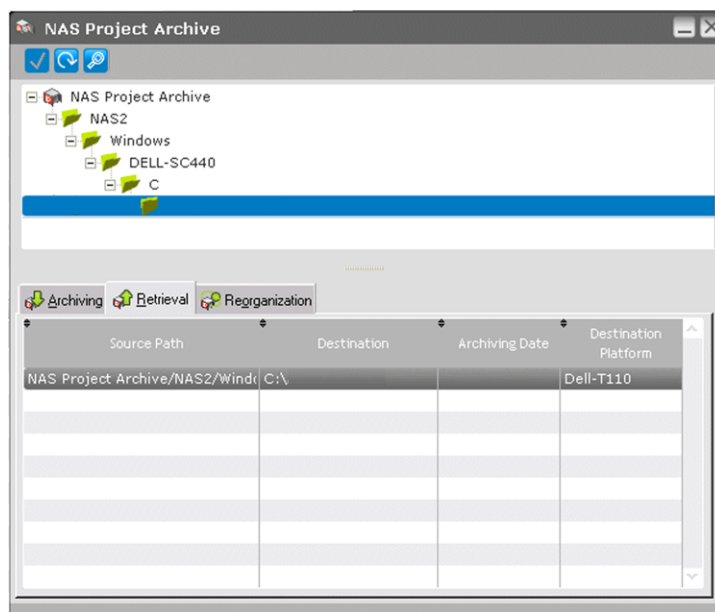



Figure 28: Selected files in the Retrieval table

9. On the Project Archive Contents window, click .
10. On the confirmation message that opens, click Yes.
Miria creates the retrieval job, which will run as soon as resources are available.
11. To close the Project Archive Contents window, click the [X] in the title bar.
12. To monitor the retrieval job, on the left pane of the Administration Console, click Jobs.
The List of Jobs window opens.
13. In the Current table, look for a job with the Action Retrieval.
Initially, the Job Status is In queue. Once it begins, the status updates to Running. Finally, when the job completes, it is moved to the History table with a Job Status of Completed.
14. To verify, check for the retrieved files in the destination folder you chose.

CHAPTER 8 - Use Case #2 - Archiving Data to NAS

This topic provides a step-by-step guide for configuring Miria to archive data from disk to network attached storage (NAS), and then retrieve it from archived storage.

For details, see the Administrator Documentation, as well as the documentation for your NAS.

System Requirements

Before you begin this procedure, ensure that both your NAS and Miria meet these initial requirements.

CIFS/SMB NAS

The CIFS/SMB NAS requires a shared directory to which you want to archive data. The shared directory must exist before you configure Miria, and it must be accessible by a UNC path. For example: `\\ServerName\Share`. Do not use a drive mapping, because the mapping is associated with a specific user and will not be accessible by Miria. When you configure Miria for archiving, you will specify the name of a user who has full permission to that share.

Miria

These are the Miria requirements:

- License to install and use Miria.
- Miria Server installed on any supported operating system. This guide uses a Windows server installation as an example.
- Miria Agent on the server with full permission to the NAS on which you want to archive data.
- Administration Console installed on a workstation or server with a connection to Miria Server.
- At least one user with full permission to Miria Server. This user is called the Super User; in this procedure, the user is root. For more information on working with users, see the Administrator Documentation.

Naming

In this topic, these names will be used in the examples to identify the required Miria objects. To simplify your configuration, you can substitute your own names and note them in this table:

Object	Name	Your Name
Source Agent (Archiving Platform)	Dell-T110	

Object	Name	Your Name
Source data location	C:\ADASource C:\MiriaSource	
Destination Agent (Archiving Platform)	dell-sc440	
NAS Archiving Platform	NAS1	
Storage Manager	Storage Manager for NAS1 on NAS	
Storage Manager Container	SMC for NAS1 \\NAS1\Storage	
Retention Period	Month	
Archiving Policy	My Archiving Policy	
Project Archive	My Project Archive	
Task	Archive MiriaSourceToMyProject	

Data Flow Diagram

This diagram ([Figure 29](#)) shows the component configuration when you configure Miria to archive data from a file server disk to NAS:

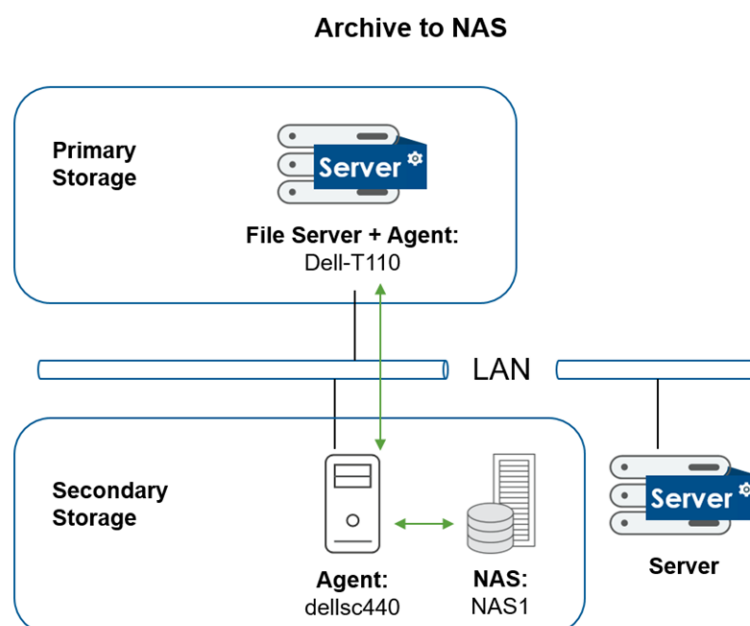


Figure 29: Component configuration to archive data from a file server to a NAS

Configuring Miria to Archive to NAS

Any time you configure archiving, you must specify the archiving source, which is the primary storage from which data will be archived, and the archiving destination, which is the secondary storage where it will be stored.

You must also configure archiving policies to determine where data will be archived and how long it will be retained.

Process Overview

In Miria, this process includes these steps:

1. [Connecting to the Administration Console.](#)
When you first log on to the Administration Console, you must specify the Miria server and database instance that you want to reach.
2. [Configuring the Archiving Source.](#)
The first step in archive configuration is to identify the source from which you want to archive files. You must install the Miria agent on that primary storage server, and then declare that Agent within Miria, so that it recognizes the location of the source. In Miria, this agent location is called the source Archiving Platform.
3. [Configuring the Archiving Destination.](#)
Once you have configured the source of archiving, you must configure the archiving destination—the secondary storage server on which archived data will be stored. In Miria, the archiving destination is defined by both the storage manager, which is the server on which data will be stored, and the storage manager container, which is a named location on the storage manager.
In this procedure, you specify the NAS as the storage manager. Since data will be stored on this server, you must also declare the NAS as an archiving platform.
4. [Creating the Retention Period.](#)
The retention period determines how long archived data are saved.
5. [Creating the Archiving Policy.](#)
This archiving policy associates the storage manager container, where archived data will be stored, with a retention policy. The result is an archiving policy that determines how long data will be retained on a given storage manager container.
6. [Creating the Project Archive.](#)
The project archive grants one or more users permission to archive and retrieve data.

The remainder of this section provides step-by-step instructions for completing each of these procedures.

Note: Miria provides smart defaults for many advanced configuration parameters. The procedures in this section make use of these smart defaults and describe only the new information or minor changes required. To learn more about the advanced settings available, see the Administrator Documentation.

Connecting to the Administration Console

In this procedure, you launch Administration Console for the first time by specifying the name of the Miria Server to which you want to connect.

This guide uses a Windows installation as an example.

To log in to the Administration Console

1. Select Start › Programs › Miria › Miria Administration Interface.
The Login window opens.
2. Enter these parameters:
 - **User.** Enter `root`.
 - **Password.** Leave this field blank.
 - **Connect in Super User Mode.** Select this box.
 - **Miria Server.** Enter your Miria server machine name.
If you modified the default port for Apache http connection (`80`) during Miria custom installation, add this custom port to the server name.
The format is:
`server_name:port_number`
For instance, if you chose port `85` instead of `80`, and the server name is `adadoc`, enter `adadoc:85` in the Miria Server field.
 - **Database Name.** Choose the database instance, by default, `Miria`.
 - **Proxy I/O Domain.** Leave this field empty.
 - **Debug.** Leave this option set to `None`.
3. Click Login.
The Administration Console opens.

The next time you launch the Administration Console, you will be automatically connected to the server and database instance that you specified here.

Configuring the Archiving Source

In this procedure, you configure Miria to archive data from disk. To do so, an Agent must be available on the primary storage server where the data is located. You declare that server as an Archiving Platform, thereby enabling Miria to recognize the location as an archive source.

To declare the source archiving agent

1. Run the Administration Console (Figure 30).

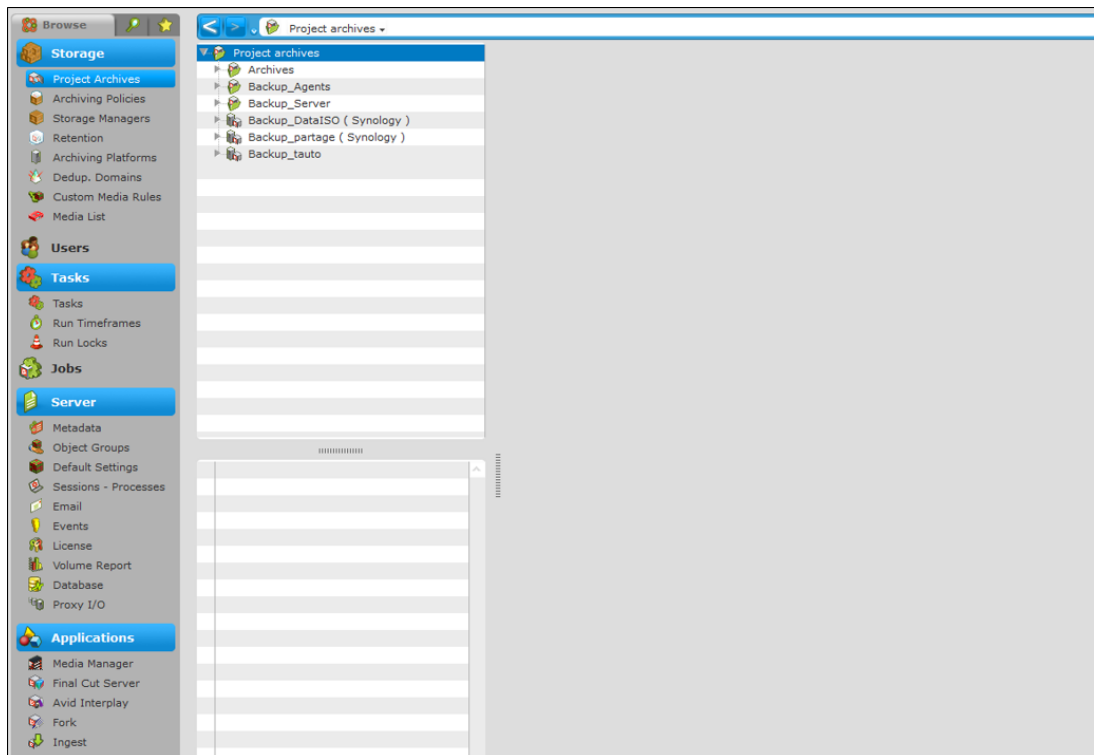


Figure 30: Administration Console interface

2. On the left pane, under Storage, click **Archiving Platforms**.
3. On the confirmation message that opens, click **Yes**.

Note: If you have already set up at least one archiving platform, then the Archiving Platforms page opens in the right pane. Click New **[+]** > **New Archiving Platform**.

The Platform Configuration window opens (Figure 31).

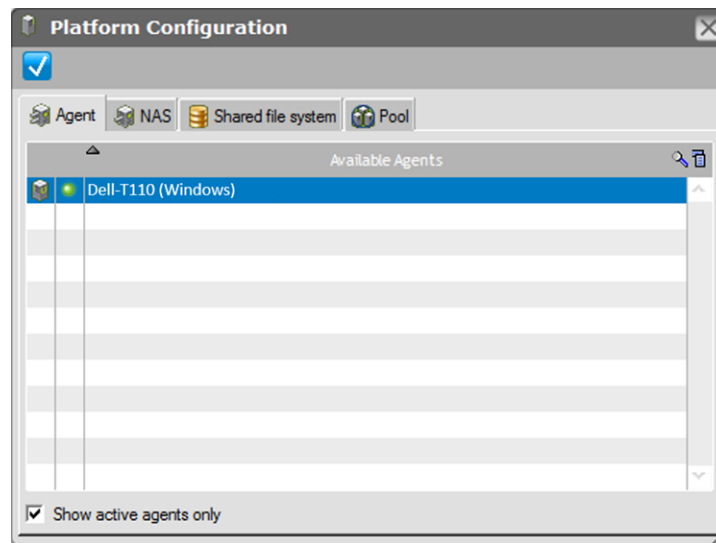


Figure 31: Source archiving agent configuration

4. Select the Configure an Agent option.
5. The Available Agents list displays one or more agents, including the agent that is installed by default with the Miria Server. Choose the agent located on the primary storage that contains the source data.

In this example, the source system is Dell-T110.

6. To accept these changes, click ☒ in the upper left corner. The Platform Configuration dialog box closes, and the Platform Properties page opens (Figure 32).

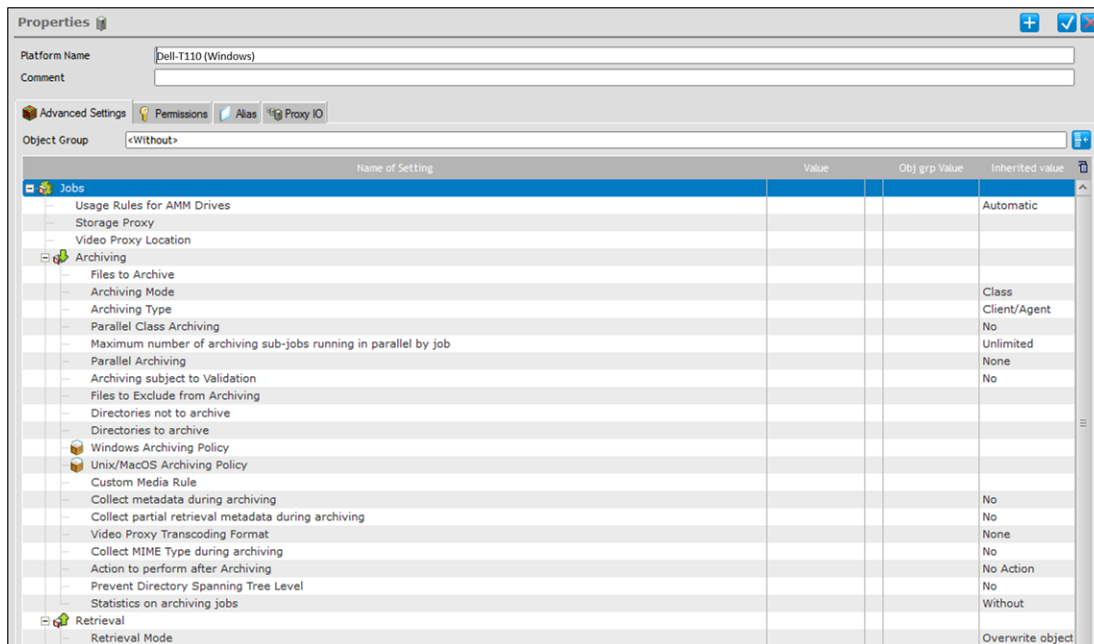


Figure 32: Source archiving agent properties

7. Keep the default configuration parameters specified in the Advanced Settings table.

8. Click ☒.

Configuring the Archiving Destination

After you have configured the source as an archiving platform, you must create the storage area on the secondary storage device. This storage area acts as the archiving destination. This process consists of two steps:

- [Declaring the Destination Location as an Archiving Platform.](#)
- [Configuring the Destination Location as Archive Storage.](#)

Declaring the Destination Location as an Archiving Platform

Since you cannot install the Miria Agent directly on NAS, you must ensure that the Miria Agent is available on the system with full access to the NAS location (share) that Miria will use to archive data.

Then, when you configure the archive destination, you declare the destination server as an Archiving Platform by identifying the Miria Agent that will act as a proxy for archiving and retrieval operations.

To declare the destination archiving agent

1. On the left pane, under **Storage**, click **Archiving Platforms**.
2. On the **Archiving Platforms Properties** page, click New [+] > **New Archiving Platform**. The **Platform Configuration** window opens ([Figure 33](#)).

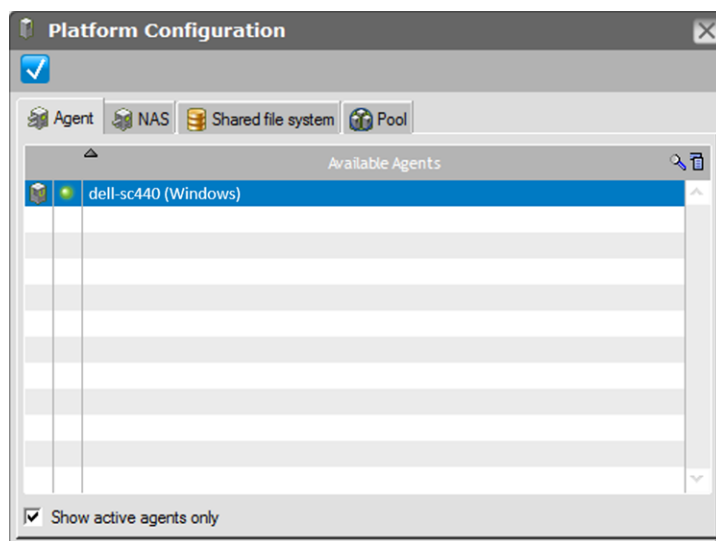


Figure 33: Destination archiving agent configuration

3. From this list, choose the agent that will act as a proxy to the NAS as the archive destination.
In this procedure, the proxy agent is `dell-sc440`.
4. To accept these changes, click ☒ in the upper left corner.

The **Platform Configuration dialog box** closes, and the Platform Properties page opens (Figure 34).

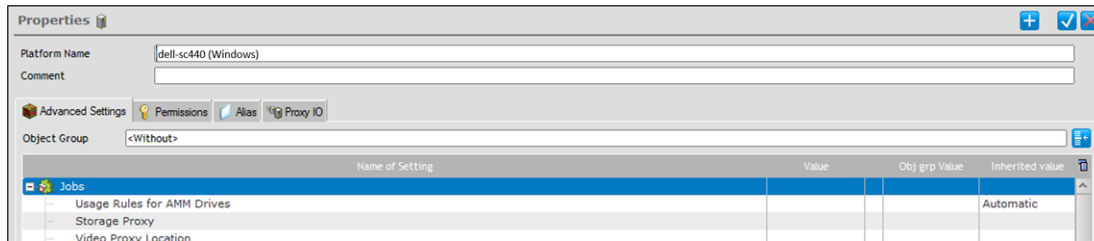



Figure 34: Destination archiving agent properties

5. Keep the default configuration parameters specified in the **Advanced Settings** table.
6. Click .

To configure the NAS as the archiving destination

1. On the left pane, under **Storage**, click **Archiving Platforms**.
2. Click New  > **New Archiving Platform**.

If the **No Miria Agent available** message displays, click **OK**. In this procedure, you are configuring the NAS, not the Agent.

The Platform Configuration window opens (Figure 35).

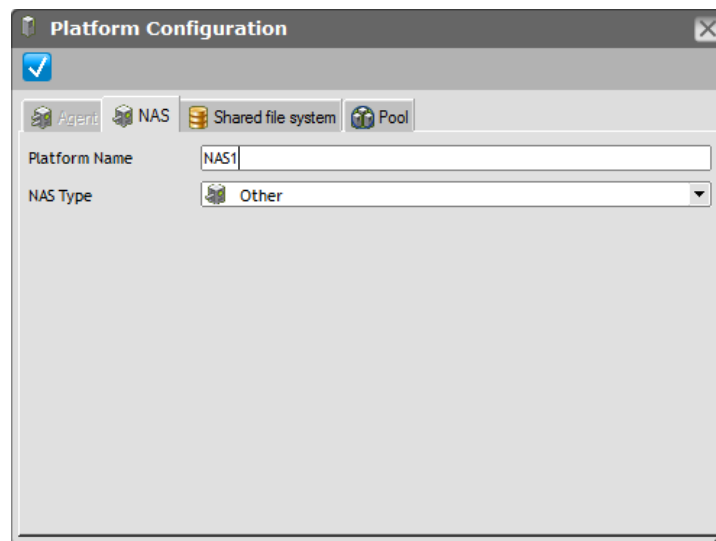



Figure 35: NAS archiving destination configuration

3. Select the **NAS** tab.
4. In the **Platform Name** box, specify the network name assigned to the NAS archiving platform you are creating.
Miria will use this platform name to access the NAS, so TCP/IP must be able to resolve this name to the IP address.
In this procedure, the Platform Name is **NAS1**.
5. From the NAS Type drop-down list, choose Other. For more information on other options in this list, see the Administrator Documentation.
6. Click  to create the **NAS Archiving Platform**. The Properties page is displayed.

7. Enter the parameters on the **NAS Properties** page:
 - a. Under **Stream Type to Process**, select the check box beside the network protocol used by the Miria agent to connect to the NAS. Note that Miria enables you to choose only the stream type that is supported by the agent. In this example, a Miria agent installed on a Windows server is in charge of data movement to the NAS, so select Windows (CIFS). If the agent was installed on Linux or macOS, you would choose Linux/macOS (NFS).
 - b. **Miria Agent** Select the agent that you specified in the [To declare the destination archiving agent](#) procedure.
 - c. **Session User** Type the name of an existing user who has read/write access to the share on the NAS.
 - If the shared directory is declared within a domain, specify the domain as part of the username (e.g., DOMAIN\Username). If the shared directory is declared within the NAS itself, then no domain specification is required.
 - d. **Password** Type the password for the specified user.
 - e. **Confirm Password** Retype the password for the specified user.
 - f. **Stream Option** Leave this option blank.
8. Click ☒ to validate the properties.

Configuring the Destination Location as Archive Storage

Once you have configured the agent that will write to the archive destination as an archiving platform, you must define a storage manager (i.e., the archive destination) and a storage manager container (i.e., the directory on the archive destination).

To create the storage manager

1. On the Administration Console, under **Storage**, click **Storage Managers**.
2. On the confirmation message that opens, click **Yes**.

Note: If you have already set up at least one storage manager, then the Storage Managers page opens in the right pane. Click New **[+]** > **New Storage Manager**.

The **Storage Manager** window opens.

3. In the **Storage Manager Name** box, type a name for the storage manager you are creating. Use a descriptive name that you can reference easily in the remaining archive configuration. In this procedure, the name is `Storage Manager for NAS1 on NAS`.
4. From the **Type** list, keep **File Storage One to One**.
This option organizes archived data in a tree structure that mirrors the data on the source file system. One directory or file on the source file system corresponds to the same directory or file on the destination file system.
5. To ensure that archiving will be active, in the Status drop down, leave the default option, **Online**.
6. On the Configuration page under Miria **File Storage One to One**, click the select button beside the **Storage Platform** box .

The Platform list opens (Figure 36).

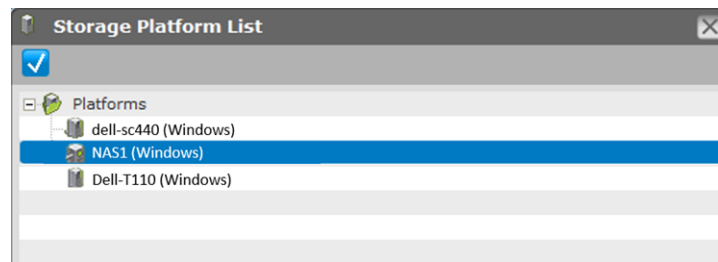




Figure 36: Destination archiving platform list

7. From the **Platform List**, select the archiving platform you created for the NAS, in this procedure **NAS1**.
 8. Click .
 9. On the **Storage Manager Properties** page, click .
- The storage manager you created opens in the **Storage Manager list** (Figure 37).

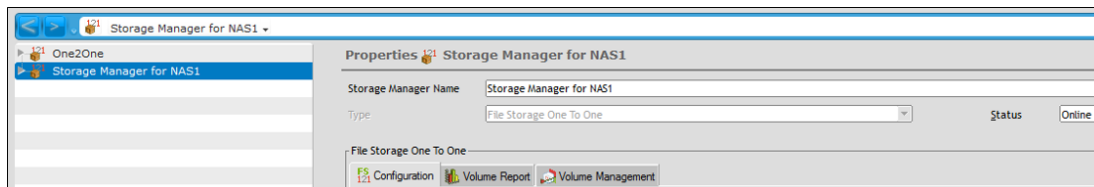


Figure 37: Newly-created storage manager

You can now create the storage manager container, which will specify the directory location where archived files will be stored.

To create the storage manager container

1. On the Administration Console, under Storage, click **Storage Managers**.
The **Storage Manager** window opens.
2. On the **Navigation** pane, right-click the **Storage Manager** that you just created and then select **New Storage Manager Container** (Figure 38). The **Storage Manager Container Properties** pane opens.

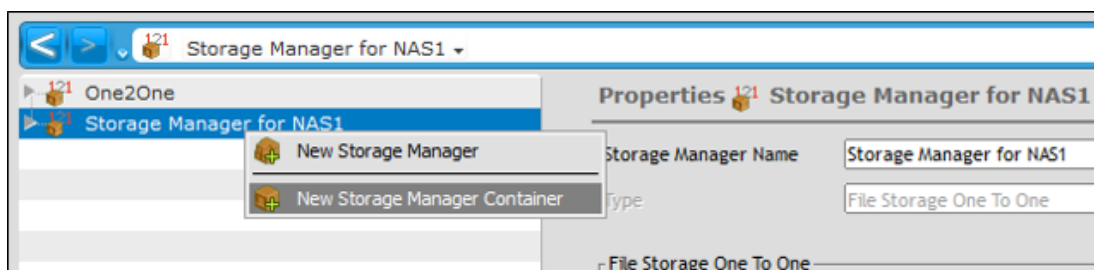

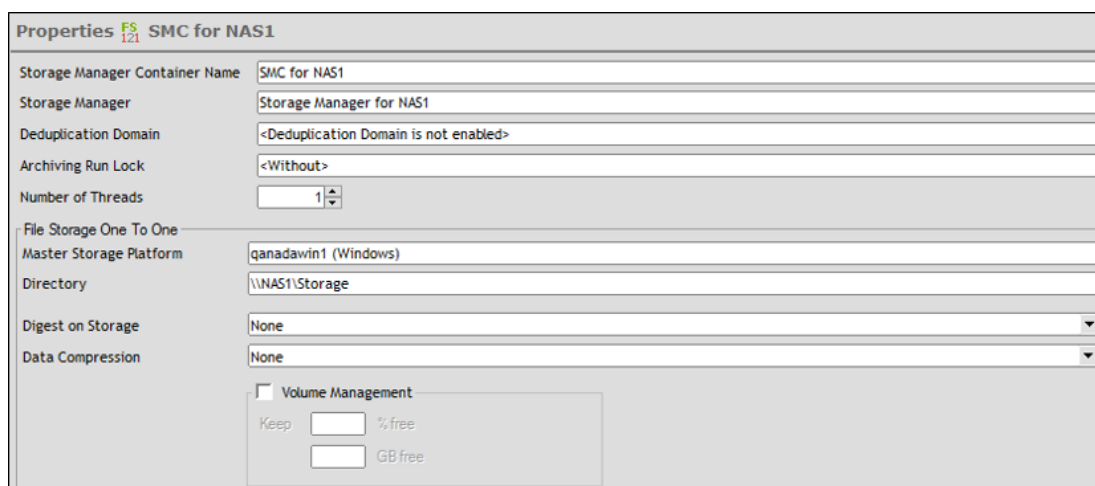


Figure 38: Create a new storage manager container

3. In the **Storage Manager Container Name** box, type a name for the container.
Use a descriptive name that you can reference easily in the remaining archive configuration.
In this procedure, the name is **SMC for NAS1**.

4. The **Storage Manager** box displays the name of the selected **Storage Manager**.
You cannot edit this name.
5. Leave the **Deduplication Domain** blank.
6. From the **Run Lock list**, choose <without>.
7. Under **Miria File Storage One to One**, the Master Storage Platform displays the archiving platform name that you created earlier and associated with the storage manager.
You cannot edit this name.
8. In the **Directory** box, type UNC path to specify the directory absolute path where the data will be archived on the storage manager.
You must create this directory on the file system and ensure that it is shared and accessible before configuring Miria to recognize it as a storage manager container.
In this procedure, the path is `\\NAS1\Storage`.
9. From the **Digest on Storage list**, choose **None**.
10. From the **Data Compression list**, choose **None**.
11. Click .

This image displays the properties of the SMC for NAS1 storage manager container once you have configured it ([Figure 39](#)).




Properties  SMC for NAS1	
Storage Manager Container Name	SMC for NAS1
Storage Manager	Storage Manager for NAS1
Deduplication Domain	<Deduplication Domain is not enabled>
Archiving Run Lock	<Without>
Number of Threads	1
File Storage One To One	
Master Storage Platform	qanadawin1 (Windows)
Directory	\\NAS1\Storage
Digest on Storage	None
Data Compression	None
<input type="checkbox"/> Volume Management Keep <input type="text"/> % free <input type="text"/> GB free	

Figure 39: Configured storage manager container

Creating the Retention Period

After you have configured both the archive source as an archiving platform, and the destination storage manager container, you must define a retention period. The retention period defines the period of time that the archived data will be saved on your storage manager before it is deleted.

To define the retention period

1. On the Administration Console, under **Storage**, click **Retention**.
2. On the confirmation message that opens, click **Yes**.
3. If you have already set up at least one Retention Period, then the Retention Period Properties page opens in the right pane. Click New **[+] > New Retention**.

The Retention Properties pane opens ([Figure 40](#)).

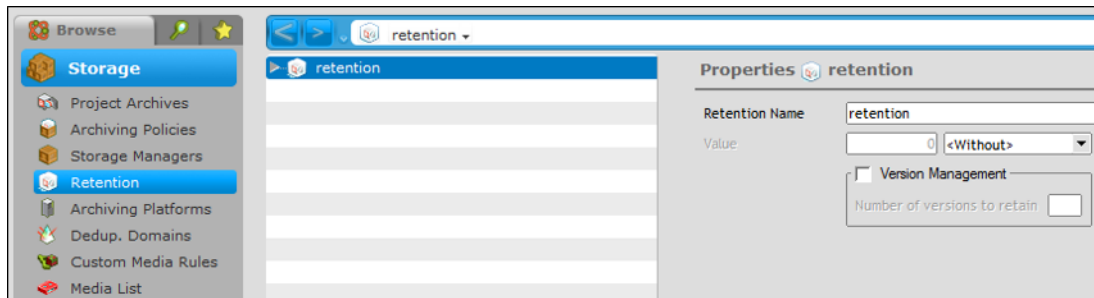



Figure 40: Retention properties

4. In the Retention Name field, type a name for the retention period.
Again, use a descriptive name, as you will specify this retention period in subsequent configuration steps.
In this procedure, you are configuring Miria to retain data for one month, so the name is **Month**

Note: By default, data is retained permanently—it is never deleted. This configuration is represented by a blank Value and <Without> selected in the drop down list.

5. To define a specific retention period, choose a unit of time from the drop-down list: Days, Weeks, Months, or Years.
6. Then type the number of that unit you want to retain the data into the Value box.
For this example, choose **Months** from the drop down list and type **1** in the Value box.
7. Click .

Creating the Archiving Policy

Now that you have created both a storage manager container, for housing the archived files, and a retention period to dictate how long archived files are saved, you can create an archiving policy. The archiving policy associates a storage manager container with a retention period, thereby defining how long archived data is retained on a particular system.

To create the archiving policy

1. On the Administration Console, under **Storage**, click **Archiving Policies**.
2. On the confirmation message that opens, click **Yes**.

Note: If you have already set up at least one Archiving Policy, then the Archiving Policy Properties page opens in the right pane. Click New  **New Archiving Policy**.

3. In the **Archiving Policy Name** box, type a name for the policy. In this procedure, the name is **My Archiving Policy**.
4. In the **Comment** box, type a description of this archive policy, (e.g., **Archiving for one month on the NAS**).
5. Beside the **Retention Name** box, click the **Select** button.

The **List of Retention Periods** window opens (Figure 41).

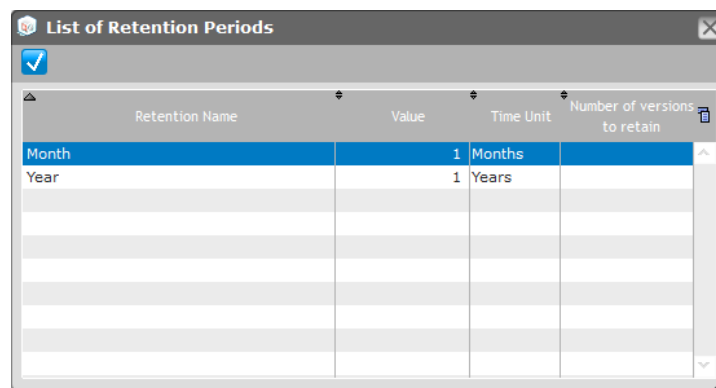


Figure 41: List of retention periods

6. Click the **Retention Period** you created in the previous procedure, and then click ☒. The retention period you have selected now displays in the Retention Name box.
7. Beside the **Storage Manager Container List**, click the [+] button. The **List of Storage Manager Containers** window opens (Figure 42):

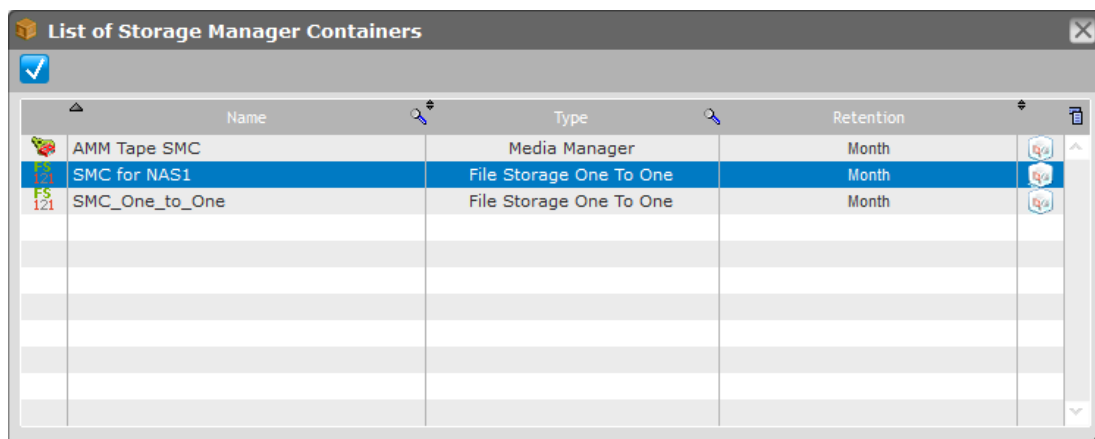


Figure 42: Storage manager container list

8. Select the storage manager container name that you want to associate with the selected retention period to create an archiving policy.
9. Click ☒. The storage manager container now displays in the List under the Archiving node:
10. On the Archiving Policies Properties pane, click ☒. The policy is created (Figure 43).

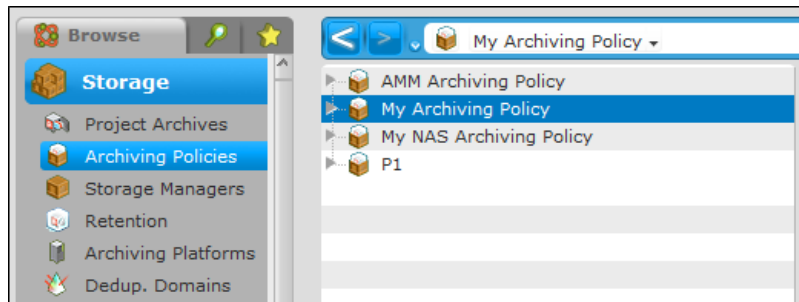


Figure 43: Archiving policy

Creating the Project Archive

The final step in the storage configuration process is to create the Project Archive. The project archive represents the container in Miria through which you can access archived data using the Miria Administration or User Interface. You will also use the project archive to set up a task to archive data. You can also assign user permissions to manually archive data.

To create the project archive

1. On the Administration Console, under **Storage**, click **Project Archives**.
2. Right-click the **Project Archives** list in the center pane, and then click **New Project Archive** (Figure 44).

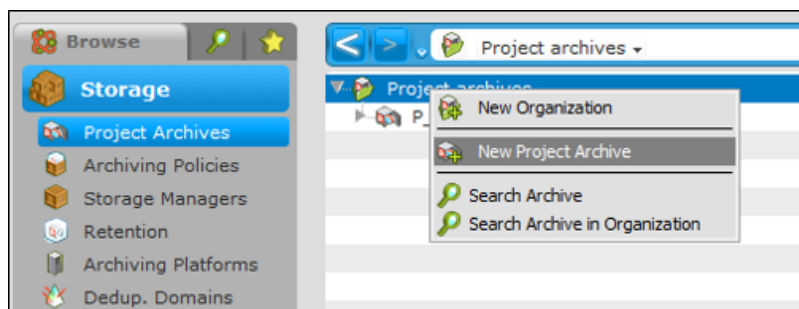


Figure 44: New project archive selection

3. In the **Project Archive Name** box, type a name for this project archive. In this procedure, the name is **My Project Archive**.
4. Beside the **Owner** box, click the **Select** button.

The **List of Users** window opens (Figure 45):

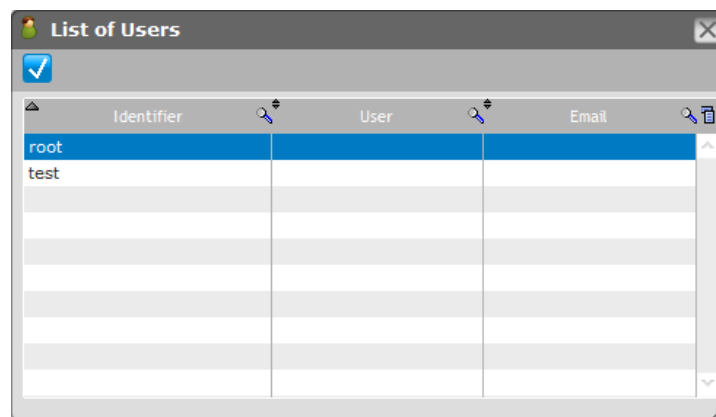



Figure 45: List of users

5. Select the `root` user, and then click  to close the window.
6. Click the **Permissions** tab. Initially, both lists on the Permissions page are disabled.
7. To enable the controls, you must add a user to whom you want to grant permissions. Click the [+] to add a user. The Selection of Users and Overall/LDAP groups list opens (Figure 46).

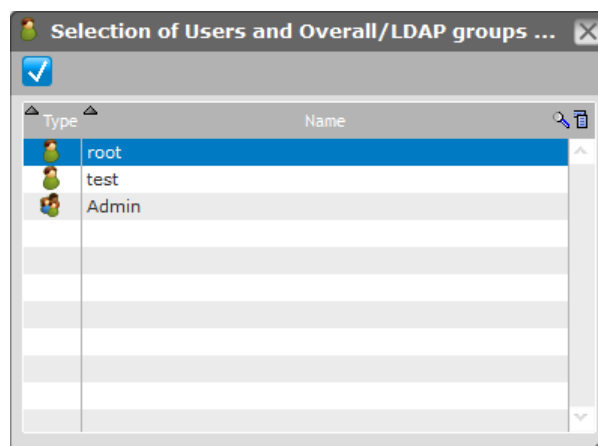



Figure 46: User and user group selection

8. From this list, select `root`, and then click .
- The `root` user opens in the User or Group Name list on the Permissions page.
9. With `root` selected in the User or Group Name list, select the Allow check box at the top of the Permissions table to grant all rights to `root` (Figure 47).

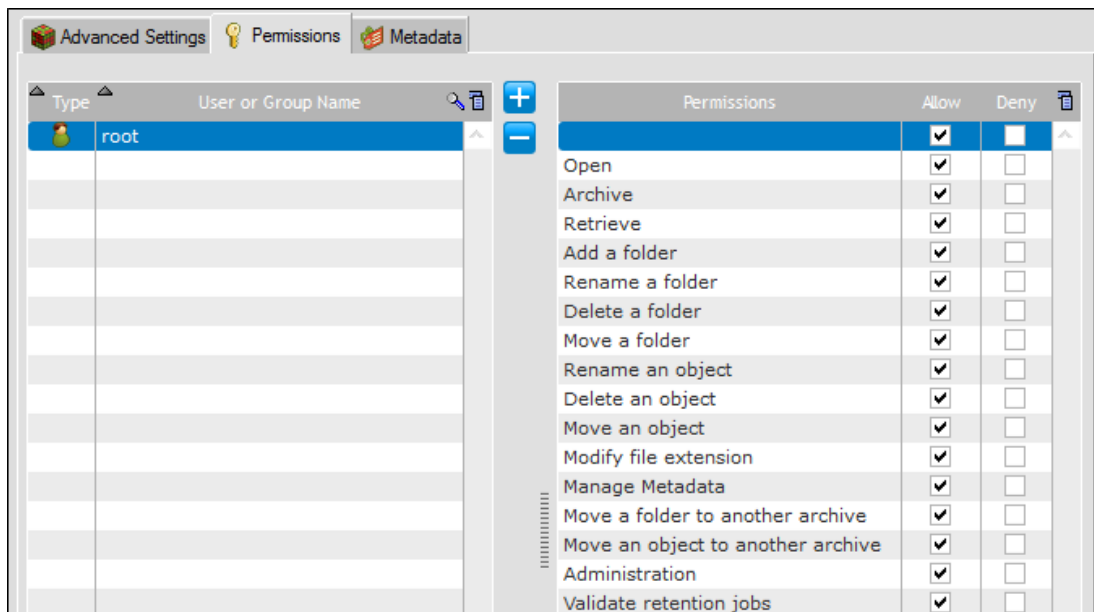


Figure 47: All rights are granted to **root**

- Click .

Creating an Archiving Task

In this procedure, you perform archiving using a named task in Miria. This configuration uses the parameters you configured in [Configuring Miria to Archive from NAS](#) to create a specific task from which you can launch and monitor the archiving job.

Note that this procedure is just one simple example of many options you have for configuring Miria. For more information on other configurations, see the Administrator Documentation.

Creating the Archiving Task

In this procedure, you create an archiving task to archive data from your preconfigured archiving platform (source) to the storage manager container (destination) based on the Automatic Archiving task template. You can select a particular path on the source archiving platform to archive, and choose a destination name for the archived data.

You will set a schedule to run the task automatically at particular times. Once the task is configured, you will perform an initial manual run. Although you run the task manually as part of these instructions, automatic scheduled runs are the typical configuration.

To create the archiving task

- On the Administration Console, under **Tasks**, click **Tasks**.
- To create a new task, on the **Task Properties** window, click **[+] > New Task**.
- From the **Template list**, select **Automatic Archiving** ([Figure 48](#)). This enables the Configuration page of Task Properties for editing, and populates the remaining advanced settings with smart defaults for your archiving task.

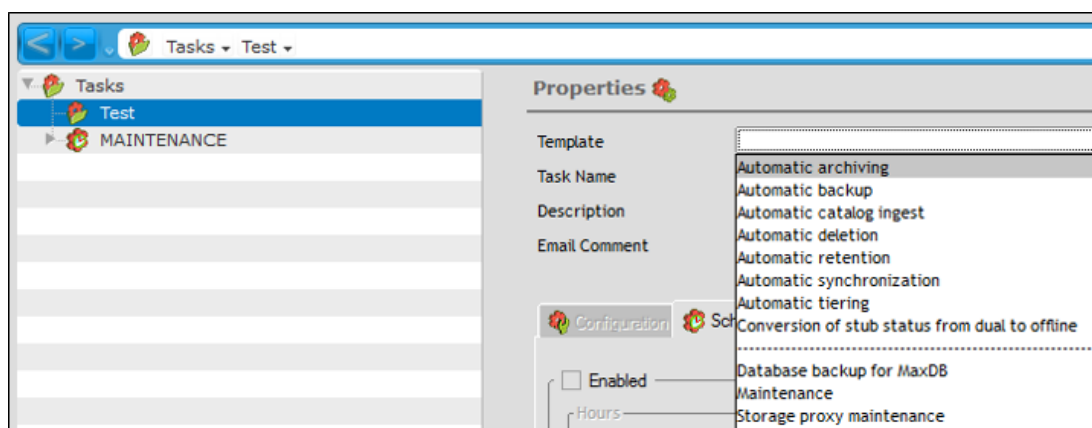


Figure 48: Automatic archiving template for a new task

4. In the **Task Name** box, type a name to identify this task within Miria.
Note that the name must not contain spaces.
In this procedure, the name is `ArchiveMiriaSourceToMyProject`.
5. In the **Description** box, type a detailed description of the task, such as `Archiving task from My Miria Source to my project archive`.
6. For now, you can leave the **Email Comment** box blank.

Note: You can use this option to specify any text you want to e-mail to authorized users when the task is triggered; however, to complete this configuration, you must also set up an SMTP Server within Miria. To learn more about configuring email notifications, see the Administrator Documentation.

7. Ensure that the **Configuration** tab is selected.
8. Configure the Source by specifying these parameters:
 - From the Storage Platform list, choose the archiving platform you created in [Configuring the Archiving Source](#).
This is the server where the agent is installed (e.g., `Dell-T110`).
 - In the Loc of Data to Archive box, type the root of the path from where archiving should start (e.g., `C:\MiriaSource`).
This directory and all subdirectories of the specified path will be archived.
9. Under **Destination**, keep the default Archive Name (i.e., Full Path Auto-generated) and then click the select button to the right of the edit box.
The **Select an archive** window opens:
10. Choose a project archive, which in this procedure was named `My Project Archive` and click ☒. When archiving begins, Miria creates a source path mirror within the storage manager container.
11. Choose your archiving policy ([Figure 49](#)):
 - a. Click the **Advanced Settings** tab.
 - b. Under **Jobs**, click the box in the **Value** column beside Windows Archiving Policy (or Linux/macOS Archiving Policy if that is your destination operating system).
 - c. From the drop-down that opens, choose the archiving policy you created. In this procedure, the name is `My Archiving Policy`.

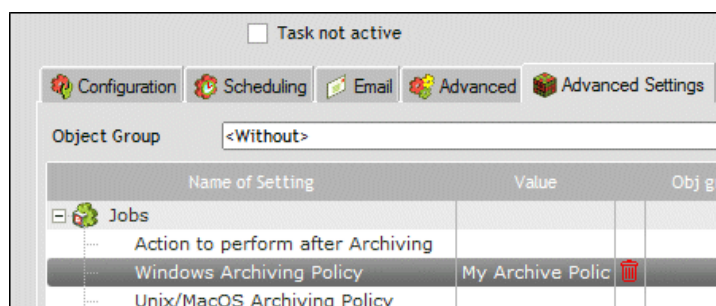


Figure 49: Archiving policy selection

12. Configure an automatic task schedule:
 - a. Click the **Scheduling** tab.
 - b. Select the **Enabled** check box.
 - c. Select the check boxes beside the Hours, Days, and Occurrences in the Month when you want to run the task. For example, to run the task the first Monday of every month at 12:00 A.M., select:
 - Hours: 12 AM
 - Minutes: 00
 - Days: Monday
 - Occurrences in the Month: 1st
 - Offset: No Offset
13. Keep all other defaults, and then click ☒.
14. On the confirmation message You have not defined any constraints. Do you want to validate anyway?, click **Yes**.
 This Task runs automatically the first Monday of next month at 12:00; however, you can test it and launch it manually beforehand to ensure that it runs properly.

Testing the Archiving Task

You can test the newly-created task before performing any actual archiving. This test verifies that Miria agent has access to the source platform and is able to select the files to archive.

To test the archiving task

1. On the **Tasks** window, in the center pane, ensure that your new task is selected.
2. Click on the microphone button to test the Task (Figure 50).

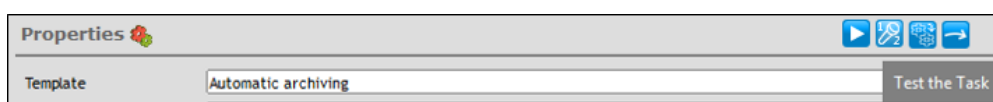


Figure 50: The microphone button is placed in the upper right corner

3. On the confirmation message that opens, click **Yes**. Miria tests the parameters of the archiving task.
4. On the confirmation message that opens, click **OK**. To validate the files and folders that will be archived as part of the task, you can review the **Event list**.

5. In the left pane of the Administration Console, select **Server > Events**. The Event List displays all the files and folders that will be archived as a result of this archiving task. If the selection is not appropriate, you can edit the Task and configure constraints. To learn more about editing task constraints, see the Administrator Documentation.

Archiving and Retrieving Data

After you have set up all of your archiving policies, and you have configured your archiving environment, you can archive and retrieve data.

In the following procedures, you archive data using the Administration Console. You can also archive and retrieve data directly from the archive source using the User Interface.

Archiving Data

Based on the task schedule you set, data will be archived automatically on Monday of the next month. To manually archive data from the Administration Console, run the archiving task that you configured in the previous procedure.

To run the archiving task

1. On the Administration Console, under **Tasks**, click **Tasks**.
2. On the center pane, in the **Tasks list**, click the task that you created in the previous procedure.
3. On the right side of the **Tasks Properties pane**, click the **Run the Task** button (Figure 51).

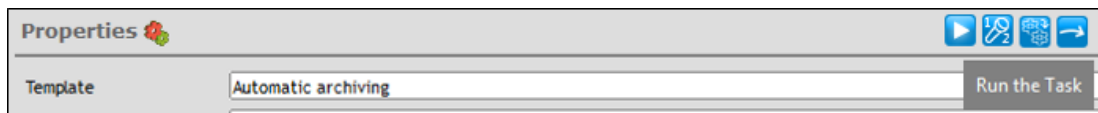


Figure 51: The Play button enables to run a task

4. On the confirmation message that opens, click **Yes**.
Miria creates the archiving job, which will run in queue as soon as resources are available. On the confirmation message that opens, click **OK**.
5. To monitor the archiving job, on the left pane of the Administration Console, click **Jobs**. The **List of Jobs** window is displayed (Figure 52).
6. In the **Current table**, under the **Action** column, look for **Task**.
Initially, the Job Status is In queue. Once the job begins to run, the status updates to Running.

Finally, when the job completes, it is moved to the History table with a Job Status of Completed.

[illegible]

Figure 52: List of jobs and their corresponding status

7. Check the destination directory on the NAS to validate that the files have been successfully archived.

You can also verify the project archive.

Note: If you see any errors during the archiving process, see the Administrator Documentation.

Retrieving a File

You can use the Administration Console to retrieve archived data. To do so, you must open the Project Archive, which contains a list of all archived data. From there, you can choose the data you want to retrieve.

If you are running Administration Console on a computer that does not have a Miria Agent installed, then you must configure a Storage Proxy to complete the Retrieval. Under **Project Archives > Advanced Settings > Jobs > Storage Proxy**, locate the Value list drop-down menu and choose an existing Storage Manager Container of the type Miria File Storage One to One, which will be used as a cache during the retrieval. If you do not have an available Miria File Storage One to One Storage Manager Container, you can create one wherever you have adequate free space. See the Administrator Documentation.

To retrieve a file

1. On the Administration Console, under **Storage**, click **Project Archive**.
2. In the list in the center pane, right-click the **Project Archive** you created and then choose **Open Archive**.

The **Project Archive** window opens and displays the contents of the archive ([Figure 53](#)).

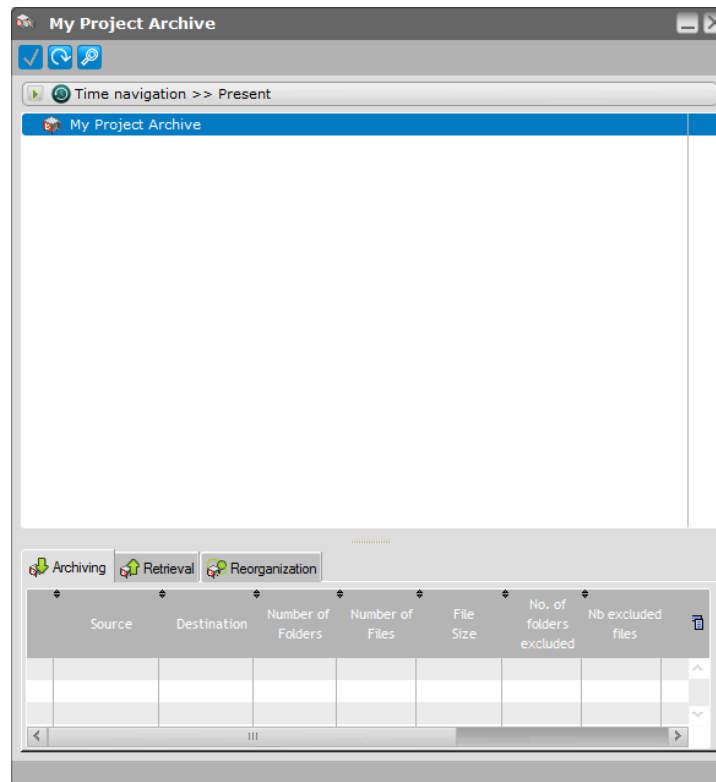


Figure 53: Archive contents

3. Expand the tree to navigate to the files that you want to retrieve.
4. To retrieve a file, right-click the file name in the tree and then choose **Retrieve**.
5. (Optional) In the **Retrieval Destination** dialog box, indicate the path of the file to retrieve in the **Source** field.
6. To the right of the **Destination** field, click on the **Browse** button. The **Browse for Folder** window opens..
7. On the local machine on which Administration Console runs, choose the path to save the retrieved data.
8. Click **OK**. The files you chose open in the Retrieval table ([Figure 54](#)).

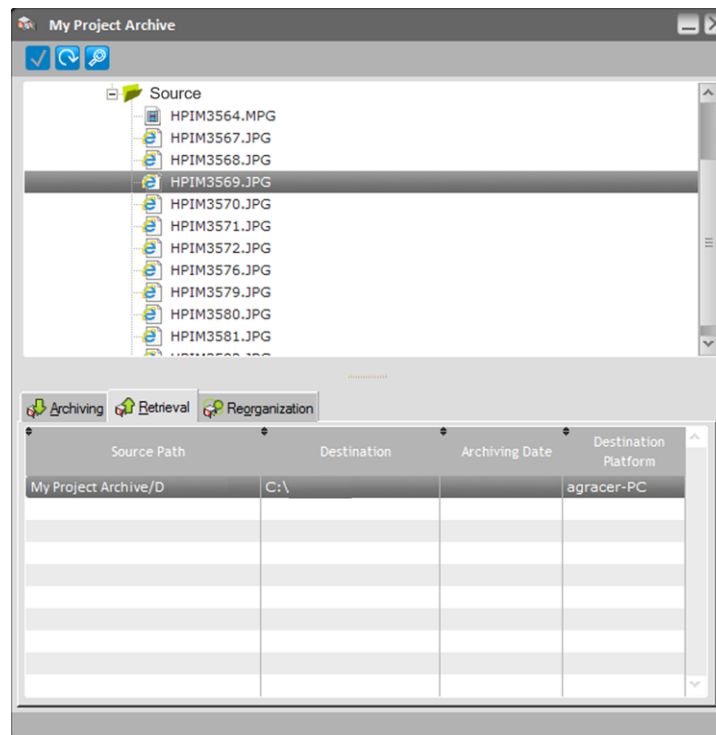



Figure 54: Selected files in the Retrieval table

9. On the **Project Archive Contents** window, click .
10. On the confirmation message that opens, click **Yes**.
Miria creates the retrieval job, which will run as soon as resources are available.
11. To close the **Project Archive Contents** window, click the [X] in the title bar.
12. To monitor the retrieval job, on the left pane of the Administration Console, click **Jobs**.
The **List of Jobs** window opens.
13. In the **Current** table, under the **Action** column, look for **Retrieval**.
Initially, the Job Status is In queue. Once the job begins to run, the status updates to Running. Finally, when the job completes, it is moved to the History table with a Job Status of Completed.
14. To verify, check for the retrieved files in the destination directory you chose.

CHAPTER 9 - Use Case #3 - Archiving Data to Tape Using Media Manager

This topic provides a step-by-step guide for configuring Miria to archive data to tape managed by Media Manager, and then retrieve that data using a simple procedure.

These steps are also covered in more detail in the Administrator Documentation.

System Requirements

Before you begin this procedure, ensure that both Miria and Media Manager meet these initial requirements.

Miria

These are the Miria requirements:

- License to install and use Miria.
- Miria Server installed on any supported operating system. This guide uses a Windows server installation as an example.
- Administration Console installed on the Miria Server.
- At least one user with full permission to Miria Server. This user is called the Super User; in this procedure, the user is *root*. For more information on working with users, see the Administrator Documentation.

Media Manager

These are the Media Manager requirements:

- Media Manager installed on any supported operating system with a tape library attached. Media Manager is installed as a Miria setup option.

This documentation uses a Windows server installation as an example with Media Manager and Miria coinstalled.

If your configuration is more complex than the simple direct attachment configuration described in this topic, or if you are using a SAN, you can find installation and configuration details for both Media Manager and Miria in [Installing Miria Server](#).

- Available scratch tapes (i.e., candidate to be assigned to and used by Miria).

Naming

In this topic, these names will be used in the examples to identify the required Miria objects.

To simplify your configuration, you can substitute your own names and note them in this table:

Object	Example Name	Your Name
Source Agent (Archiving Platform)	Dell-T110	
Source data location	\\Dell-T110\c\MiriaSource	
Destination Agent (Archiving Platform)	Dell-T110	
Media Manager Application	Atempo Media Manager	
Storage Manager	Atempo Media Manager SM	
Storage Manager Container	AMM Tape SMC	
Retention Period	Forever	
Archiving Policy	AMM Archiving Policy	
Project Archive	AMM Project Archive	

Data Flow Diagram

This diagram shows the component configuration when you configure Miria to archive data from disk to tape (Figure 55).

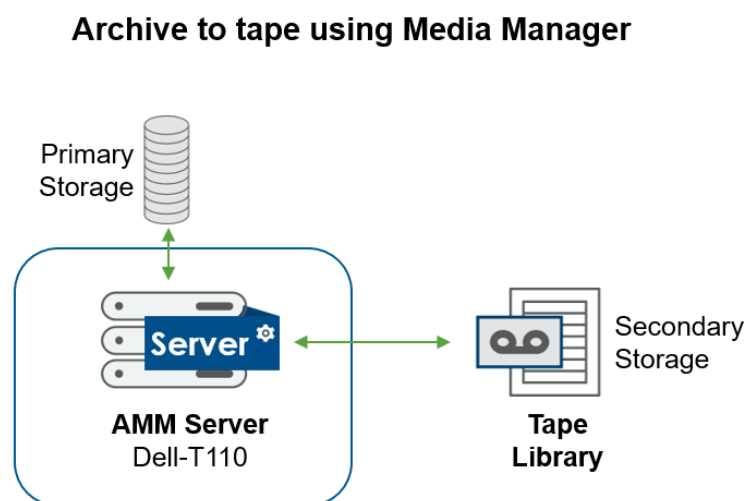


Figure 55: Configuration to archive data from disk to tape

Configuring Miria to Archive to Tape

Any time you configure archiving, you must specify the archiving source, which is the primary storage from which data will be archived, and the archiving destination, which is the secondary

storage where it will be stored. You must also configure archiving policies to determine where data will be archived and how long it will be retained.

Process Overview

In Miria, this process includes these steps:

1. [Connecting to the Administration Console.](#)
When you first log on to the Administration Console, you must specify the Miria server and database instance that you want to reach.
2. [Configuring the Archiving Source.](#)
The first step in archiving configuration is to identify the source from which you want to archive files. In this procedure, you specify a disk location as the source of archive data, or the primary storage. In this configuration, the disk location is on the Miria Server itself, so you must only declare the Miria Server as the Archiving Platform in charge of data movement from disk to tape.
3. [Configuring the Archiving Destination.](#)
After you have configured the source of archiving, you must configure the archiving destination—the secondary storage server on which archived data will be stored. In this configuration, the archiving destination is a tape library attached to the Miria Server. The tape library is managed by Media Manager Server, which is also installed on the Miria Server. You will have declared the Miria Server as an Archiving Platform in the first step; therefore, the Miria Server will manage both data movement from the primary storage and data movement to the tape. To configure the archiving destination, you must declare a Media Manager Application, then this application as the Storage Manager, and then an available tape as the Storage Manager Container.
4. [Creating the Retention Period.](#)
The retention period determines how long archived data will be saved. In this procedure, you will retain the data indefinitely.
5. [Creating the Archiving Policy.](#)
The archiving policy associates the storage manager container, where archived data will be stored, with a retention policy. The result is an archiving policy that determines how long data will be retained on a given storage manager container.
6. [Creating the Project Archive.](#)
The project archive grants one or more users permission to archive and retrieve data.

The remainder of this section provides step by step instructions for completing each of these procedures.

Note: Miria provides smart defaults for many advanced configuration parameters. The procedures in this section use these defaults and describe only minor changes required. To learn more about the advanced settings available, see the Administrator Documentation.

Connecting to the Administration Console

In this procedure, you launch Administration Console for the first time by specifying the name of the Miria Server to which you want to connect.

This documentation uses a Windows installation as an example.

To log in to the Administration Console

1. Select Start › Programs › Miria › Miria Administration Interface. The Login window opens.
2. Enter these parameters:
 - **User.** Enter `root`.
 - **Password.** Leave this field blank.
 - **Connect in Super User Mode.** Select this box.
 - **Miria Server.** Enter the name of your Miria Server machine.
 If you modified the default port for Apache http connection (80) during Miria custom installation, add this custom port to the server name.
 The format is `server_name:port_number`.
 For instance, if you chose port 85 instead of 80, and the server name is `adadoc`, enter `adadoc:85` in the `ADA Server` field.
 - **Database Name.** Choose the database instance, by default, `Miria`.
 - **Proxy I/O Domain.** Leave this field empty.
 - **Debug.** Leave this option set to `None`.
3. Click Login.
 The Administration Console opens.

The next time you launch the Administration Console, you are automatically connected to the server and database instance that you specified here.

Configuring the Archiving Source

In this procedure, you configure Miria to archive data from disk. To do so, an Miria Agent must be available on the primary storage server where the data is located. In this configuration, you archive from a disk on the Miria Server, so an Miria Agent is already available. You need only declare that server as an Archiving Platform, thereby enabling Miria to recognize the location as an archive source.

To declare the source archiving agent

1. Run the Administration Console ([Figure 56](#)).

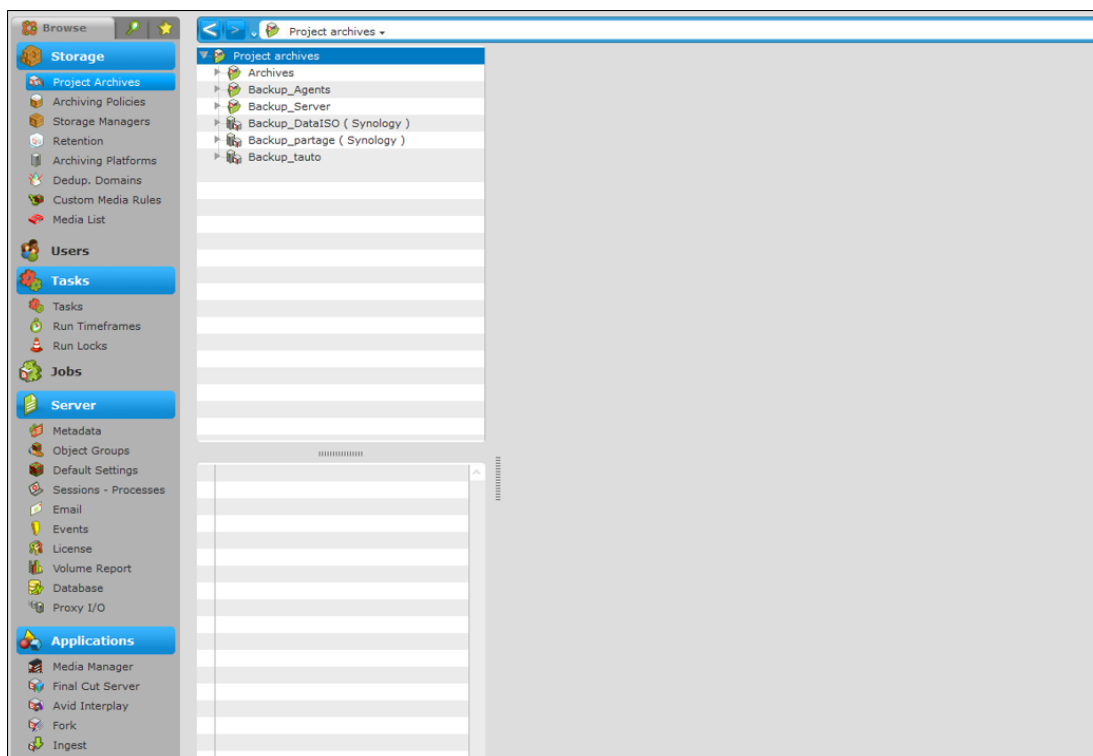


Figure 56: Administration Console interface

- On the left pane, select **Storage > Archiving Platforms**.
On the confirmation message that opens, click **Yes**.

Note: If you have already set up at least one archiving platform, then the Archiving Platforms page opens in the right pane. Click New [+] > New Archiving Platform.

The Platform Configuration window opens (Figure 57).

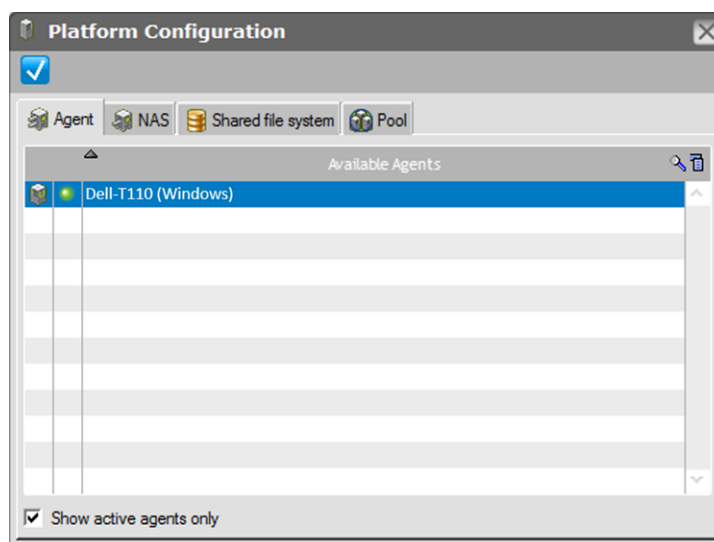


Figure 57: Source archiving agent configuration

- Select the **Configure an Agent option** button.

4. The **Available Agents list** may list one or more agents, including the agent that is installed by default with the Miria Server. Choose the agent located on the primary storage that contains the source data (i.e., the Miria Server).
In this procedure, the source system is Dell-T110.
5. To accept these changes, click ☒ in the upper left corner.
The Platform Configuration dialog box closes, and the platform Properties pane opens (Figure 58).

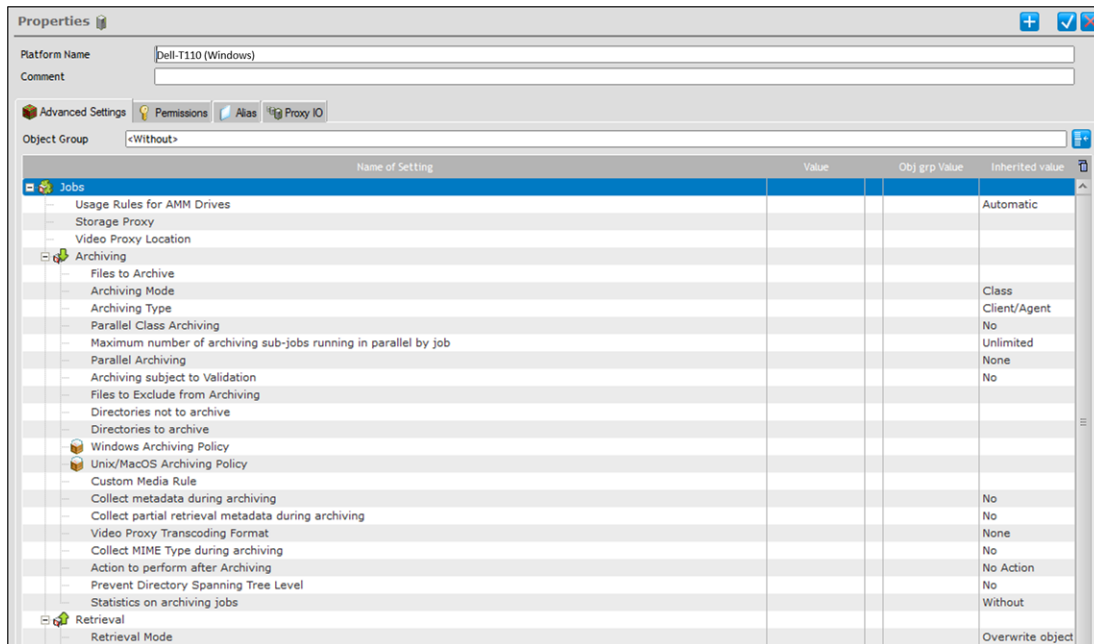


Figure 58: Source archiving agent properties

6. Keep the default configuration parameters specified in the **Advanced Settings** tab.
7. Click ☒.

Configuring the Archiving Destination

After you configure the source as an archiving platform, you must then create the storage area on the secondary storage device, which acts as the archiving destination.

This process consists of configuring a Media Manager application as the storage manager and a tape as the storage manager container.

For more information on configuring Media Manager as a Storage Manager in Miria, see the Administrator Documentation.

Configuring the Storage Manager and the Container

In this procedure, you create a Media Manager Application, define the Media Manager as the Storage Manager (the archive destination) and a tape as the Storage Manager Container.

To create a Media Manager Application

1. On the Administration Console, select **Applications > Media Manager**.

2. On the confirmation message that opens, click **Yes**. The **Storage Manager Properties** window opens.
3. In the **Application Name** box, type a name for the Media Manager Application that you are creating (Figure 59).

Use a descriptive name that you can reference easily in the remaining archive configuration steps.

In this procedure, the name is `Atempo Media Manager`.

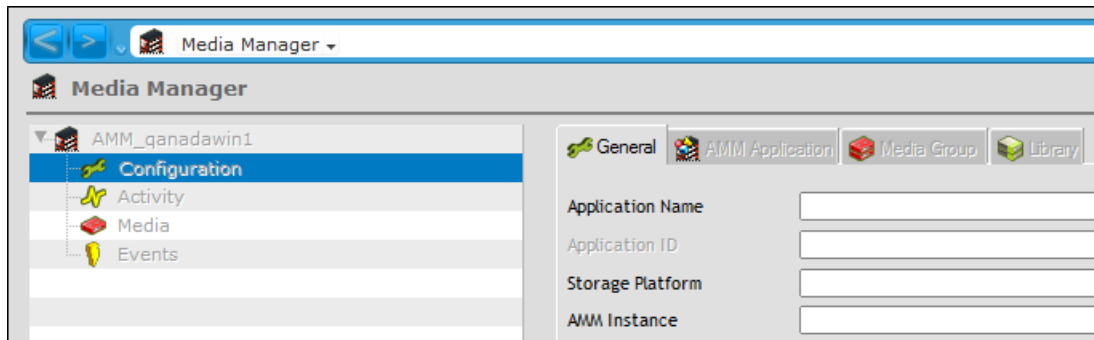


Figure 59: Properties to a Media Manager application

4. On the **General** page, click the select button beside the **Storage Platform** box. The **Platform List** window opens.
5. From the **Platform List**, select the archiving platform of the AMM Server: in this procedure `Dell-T110`.
6. Click ☒.
7. On the **General** page, click the select button beside the **AMM Instance** box. The **List of AMM Instances** window opens.
8. Select your AMM installation, and then click ☒.
9. On the **Media Manager Application Properties** pane, click ☒. The **Media Manager Application** that you created opens in the **Application list**.

Information to the Media Manager application

Notice the Application ID (). This ID is assigned automatically and cannot be changed. If the Media Manager server is available, the application Properties pane displays the Media Manager tree (Figure 60).

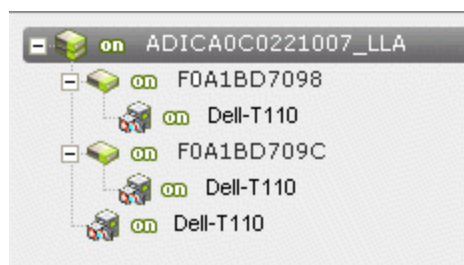


Figure 60: Media Manager tree

The Media Manager tree displays the drives, libraries, and platforms of the Media Manager configuration, along with their status and relationship to each other. It also lists the media present in each drive and their status.

For more information on Media Manager device status, see the Administrator Documentation.

You can now create the storage manager, which specifies the Media Manager application to be used to archive to tape.

Creating a Media Manager Storage Manager

Before creating a Media Manager storage manager, take into account these recommendations.

Diagnostics

These are the diagnostics that you should perform:

- **Drive.** Set of steps that are executed to check the drive and media status.
Miria selects a drive and sends a mount request to Media Manager to mount a media with *scratch* or *blank* status.
If the drive diagnostic fails:
 - The media status is reset to *scratch*. Thus, the media content is erased during the next mount request.
 - The diagnostic job exits on error.
 If the drive diagnostic successes:
 - The media content is erased. This completes the diagnostic.
 - The media status is set to *blank* in Media Manager.
 - The diagnostic job ends with success.
- **Performance.** The performances measured during the driver diagnostic should be equivalent to the native driver specifications.

Features supported

These are the features that Miria supports:

- Drive sharing between multiple Miria datamovers managed by the same Media Manager server.
Example. You may have a configuration with three drives and libraries connected at the same time to **Datamover 1** and to **Datamover 2**.
 - **Driver.** Concurrent access to drive supported and managed by Media Manager server.
 - **Library.** Automatic Load-Balancing / Fail Over of the management of the Library by datamovers.
- Can manage a library connected to Datamover only.
- Can mix the technology of drive on the same partition.
In this case, it is recommended that the library expose the media technology on the barcode (e.g., ended by L4 for LT04 Media).

To create a Media Manager Storage Manager

1. On the Administration Console, under **Storage**, click **Storage Managers**.

- On the confirmation message that opens, click **Yes**.

Note: If you have already set up at least one storage manager, then the Storage Managers page opens in the right pane. Click New **[+]** > **New Storage Manager**.

The **Storage Manager Properties** window opens (Figure 61).

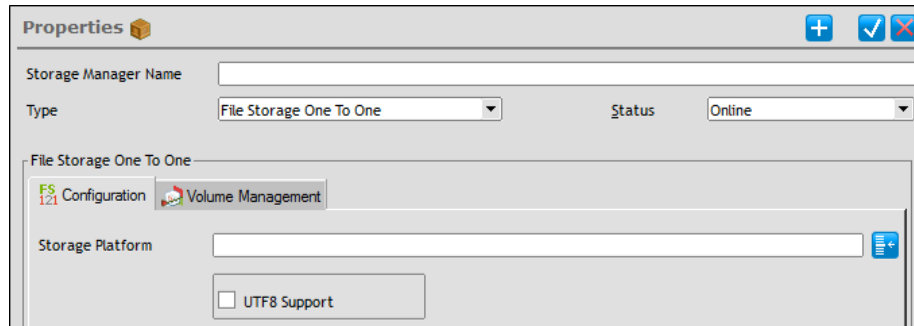


Figure 61: Storage manager properties

- In the **Storage Manager Name** box, type a name for the storage manager that you are creating.
Use a descriptive name that you can reference easily in the remaining archive configuration steps.
In this procedure, the name is **Atempo Media Manager SM**.
- From the **Type** list, choose **Atempo Media Manager**.
This option enables Media Manager to manage the tapes on which you will archive data. When you choose this option, Miria scans the system for the Atempo Media Manager installation and provides the appropriate options for the Media Manager configuration.
- To ensure archiving will be active, in the **Status** list, leave the default option, **Online**.
- On the **Configuration** page, click the select button beside the **Application** box.
The **List of Media Manager Applications** opens.
- From this **List**, select the **Media Manager Application**: in this procedure **Atempo Media Manager**.
- Click ☒.
- The **AMM Instance** field is automatically completed. It displays the instance selected when creating the Media Manager application.
- Leave the Group/User Name box empty.
- On the **Storage Manager Properties** page, click ☒.
- The Media Manager Manager storage manager that you created opens in the Storage Manager list.
You can now create the storage manager container, which specifies available media where archived data will be stored.

To create the Storage Manager Container

- On the Administration Console, under **Storage**, click **Storage Managers**.
The **Storage Manager** window opens.

- On the **Navigation** pane, right-click your newly-created storage manager, **Media Manager SM**, and select **New Storage Manager Container** (Figure 62). The **storage manager container Properties** pane opens.

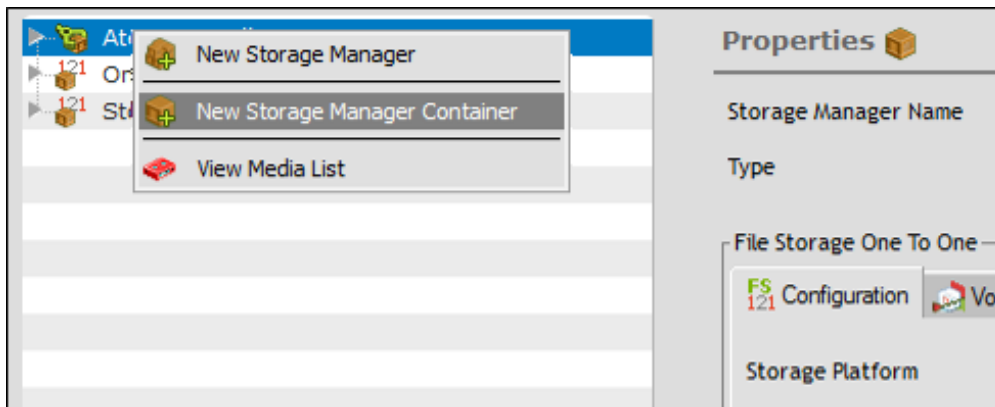


Figure 62: Context menu to create a new storage manager container

- In the **Storage Manager Container Name** box, type a name for the container. Use a descriptive name that you can reference easily in the remaining archive configuration steps. In this procedure, the name is **AMM Tape SMC**.

Note: The Storage Manager box displays the name of the selected storage manager. You cannot edit this name.

- Leave the **Deduplication Domain** field blank.
- From the **Run Lock list**, choose <without>.
- Under the **Media Manager** section, choose the options for the tape that you want to designate as the storage manager container. The tape that you choose must be available, mounted, and empty, or Scratch. The Library box defines the tape library that will be used for archiving. Beside this box, click the Select button. The Library List opens (Figure 63).

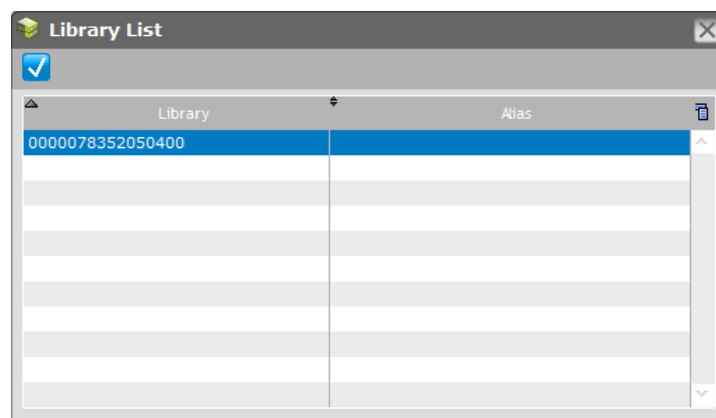


Figure 63: Library list

- Select a library and click .

8. If the library contains several types of media and that you want Miria to use only one of them, click the **Select** button and select a media type. Otherwise, leave the **Media Type** field blank.

The Scratch media group box defines the media group in which the scratch media needed for archiving is selected. Beside this box, click the Select button.

The List of Scratch Media Groups opens (Figure 64).

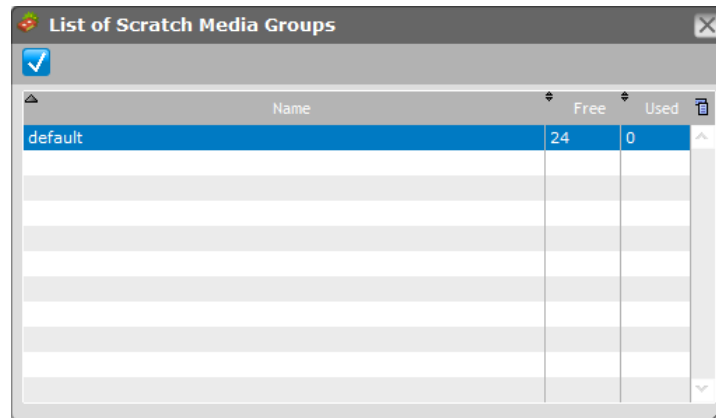


Figure 64: Scratch media groups

9. Select a scratch media group, and click ☒.
- The Barcode Selection determines which media in the group will be used. By default, Media Manager selects the first Scratch Media available in the Scratch Media Group. In this scenario, you can leave this selection blank and allow Media Manager to make the selection.
 - The Media Rule drop-down lets you choose how the data will be grouped and organized on the media during archiving. Leave this option set to **None**, which means that Miria will fill the media with archiving requests in the order they are received and will optimize space on the media.
 - From the Media Format drop-down, choose **PAX**.
This scenario does not deal with the LTFS format.
 - The Digest on Storage list determines the digest type used to ensure that the data you retrieve has not been modified from the original archived version. In this procedure, you can leave this option set to **None**. Setting a digest here is only useful in case of legal archiving.
 - The Metadata option enables to send to the storage all Miria metadata associated with the archived objects. Consider clearing this selection to save space on storage if you deal with very large volumes of data.
 - The Prevent Spanning option prevents a large file from being written to more than one disk if there is not enough room on the first one. For this procedure, you can select this option; however, if you are archiving very large files as part of your production data, consider clearing this selection during your archive deployment.
 - By default, the media is divided and written to in blocks of 128 KB. On Windows, some devices are limited to 64 KB. Therefore, in this procedure, select the Custom Block Size check box, and select 64 in the box below it.
 - Leave the Log Level list option set to **None**.

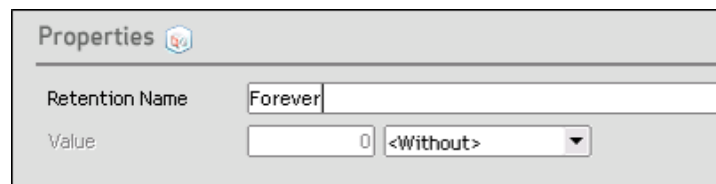
- Click ☒ to complete the configuration. The storage manager container properties are displayed.

Creating the Retention Period

After you have configured an archiving platform for the source disk, and Media Manager as the destination storage manager, you must define a retention period. The retention period defines the period of time that the archived data will be saved on your storage manager before it is deleted.

To create the retention period

- On the Administration Console, under **Storage**, click **Retention**.
- On the confirmation message that opens, click **Yes**.
- If you have already set up at least one **Retention Period**, then the **Retention Period Properties** page opens in the right pane. Click the **New [+] > New Retention**.



The screenshot shows a 'Properties' dialog box for a retention period. It has two main fields: 'Retention Name' and 'Value'. The 'Retention Name' field is a text box containing the word 'Forever'. The 'Value' field consists of a text box containing the number '0' and a dropdown menu currently showing '<Without>'.

Figure 65: Retention properties

- In the **Retention Name** box, type a name for the retention period (Figure 65). Again, use a descriptive name, as you will specify this retention period in subsequent configuration. In this procedure, you configure Miria to retain data permanently, so the name is **Forever**.
- Miria's default is to retain data permanently; therefore, leave the Value blank and the drop-down list selection set to **<Without>**.
- Click ☒.

Creating the Archiving Policy

Now that you have created both the Media Manager storage manager container and a retention period to dictate how long archived files are saved, you can create an archiving policy. The archiving policy associates a storage manager container with a retention period, thereby defining how long archived data is retained on a particular system.

To create the archiving policy

- On the Administration Console, under **Storage**, click **Archiving Policies**.
- On the confirmation message that opens, click **Yes**.

Note: If you have already set up at least one Archiving Policy, then the Archiving Policy Properties page opens in the right pane. Click **New [+] > New Archiving Policy**.

The archiving policy Properties pane opens:

- In the **Archiving Policy Name** box, type a name for the policy. In this procedure, the name is **AMM Archiving Policy**.

4. In the Comment box, type a description of this Archiving Policy (e.g., **Archive to tape and retain forever**).
5. Beside the Retention Name box, click the Select button.
The List of Retention Periods window opens:
6. Click the Retention Period you created in the previous procedure, and then click ☒.
The retention period you have selected now displays in the Retention Name box.
7. Beside the Storage Manager Container List, click the [+] button.
The List of Storage Manager Containers window opens ([Figure 66](#)).

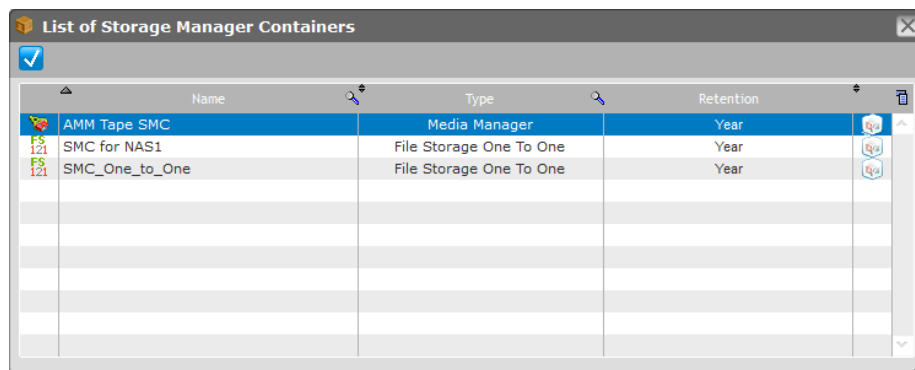


Figure 66: Storage manager container list

8. Select the name of the storage manager container that you want to associate with the selected retention period to create an archiving policy (i.e., in this procedure **AMM Tape SMC**), and then click ☒.
The storage manager container now displays in the Storage Manager Container List under the Archiving node ([Figure 67](#)).

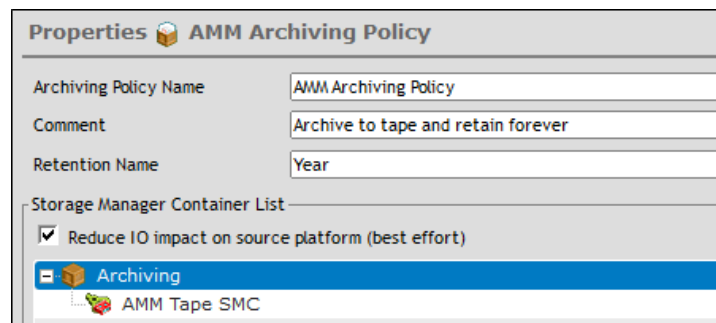


Figure 67: Configured archive policy

9. On the Archiving Policies Properties pane, click ☒.

Creating the Project Archive

The final step in the archiving configuration process is to create the Project Archive. The project archive represents the container in Miria through which you can archive and retrieve data using the Miria Administration or User Interface.

To create the project archive

1. On the Administration Console, select **Storage** > **Project Archives**.
2. Right-click the **Project Archives** list in the center pane, and then click **New Project Archive** (Figure 68).

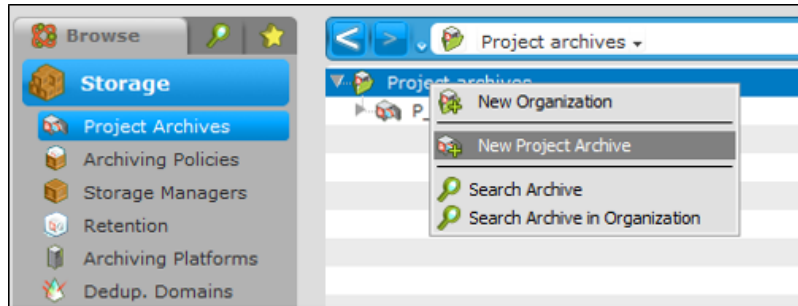


Figure 68: New project archive selection

3. In the **Project Archive Name** box, type a name for this project archive. In this procedure, the name is **AMM Project Archive**.
4. Beside the Owner box, click the **Select** button. The **List of Users** window opens (Figure 69):

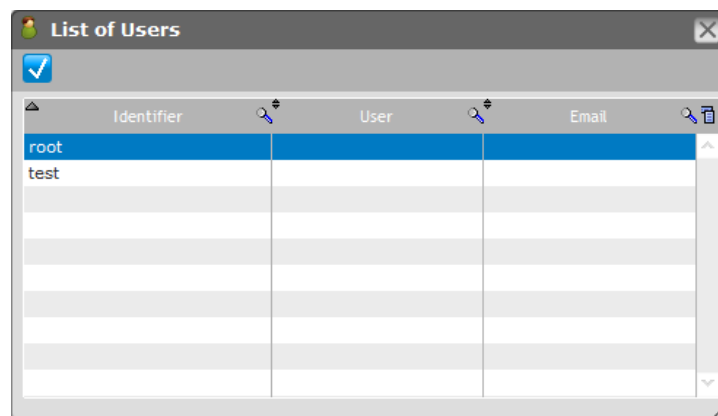


Figure 69: List of users

5. Select the **root** user, and then click ☒ to close the window.
6. Click the **Permissions** tab. Initially, both lists on the Permissions page are disabled.
7. To enable the controls, you must add a user to whom you want to grant permissions. Click the **[+]** to add a user. The Selection of Users and Overall/LDAP groups list opens (Figure 70).

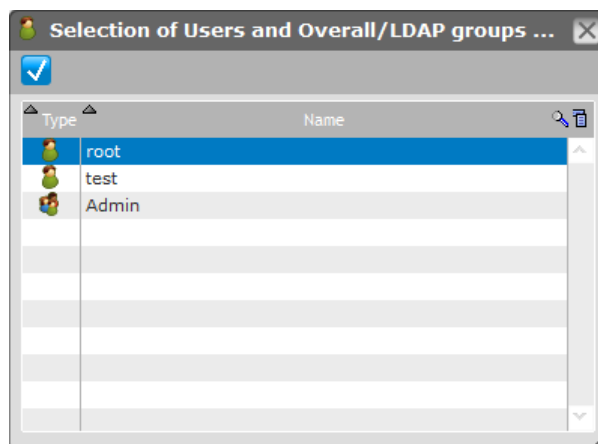
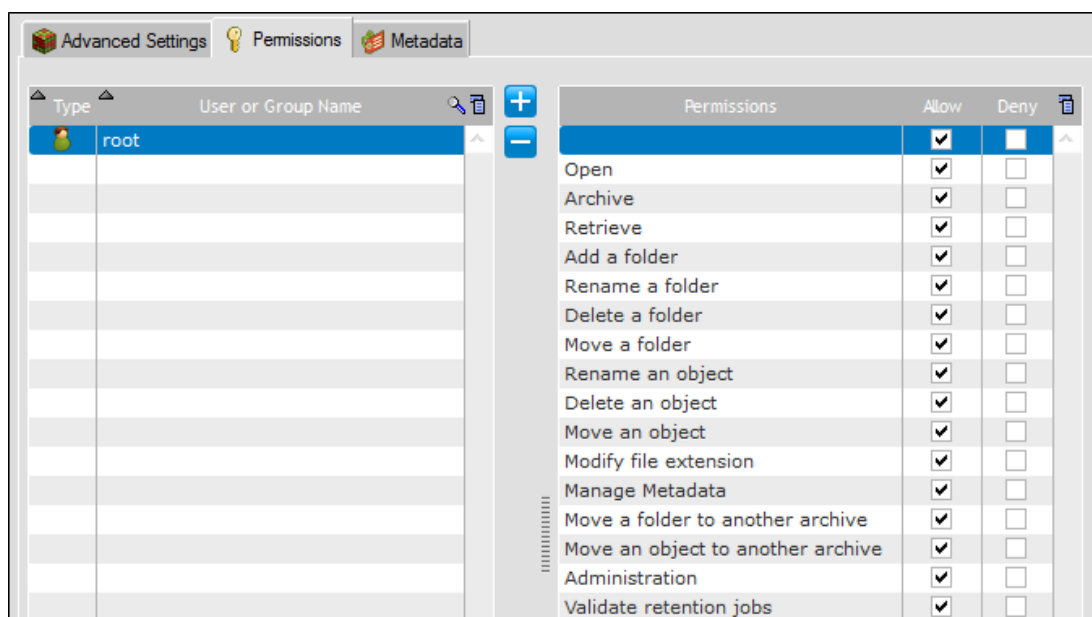


Figure 70: User and user group selection

8. From this list, select `root`, and then click ☒.
- The `root` user opens in the User Name/Group list on the Permissions page.
9. With `root` selected in the User or Group Name list, select the Allow check box at the top of the Permissions table to grant all rights to `root` (Figure 71).

Figure 71: All rights are granted to `root`

10. Click the **Advanced Settings** tab.
11. Under **Jobs**, beside **Windows Archiving Policy**, drop down the Value and choose the Archiving Policy that you created (i.e., `AMM Archiving Policy`).
12. Click ☒.

Archiving and Retrieving Data

After you have set up your Project Archive, you can archive and retrieve data.

In the following procedures, you archive and retrieve data directly from the Project Archive on the primary storage server, in this case, the Miria Server.

There are other ways you can archive and retrieve data, including setting up a task to perform automatic archiving and using the Miria User Interface.

Archiving Data

Using the Administration Console, you can archive data directly from Windows Explorer to the Project Archive you created. First open the Project Archive, then run Windows Explorer and drag any directory to the open archive to launch the archiving job.

To archive data in the Project Archive

1. On the Administration Console, click **Project Archive**.
2. Right-click the AMM Project Archive, and choose **Open Archive**.
The **AMM Project Archive** opens. You can use this archive to archive, retrieve, and reorganize data.
3. Run Windows Explorer and navigate to the directory that contains the data that you want to archive.
4. Drag the folder from Windows Explorer to the AMM Project Archive window ([Figure 72](#)).

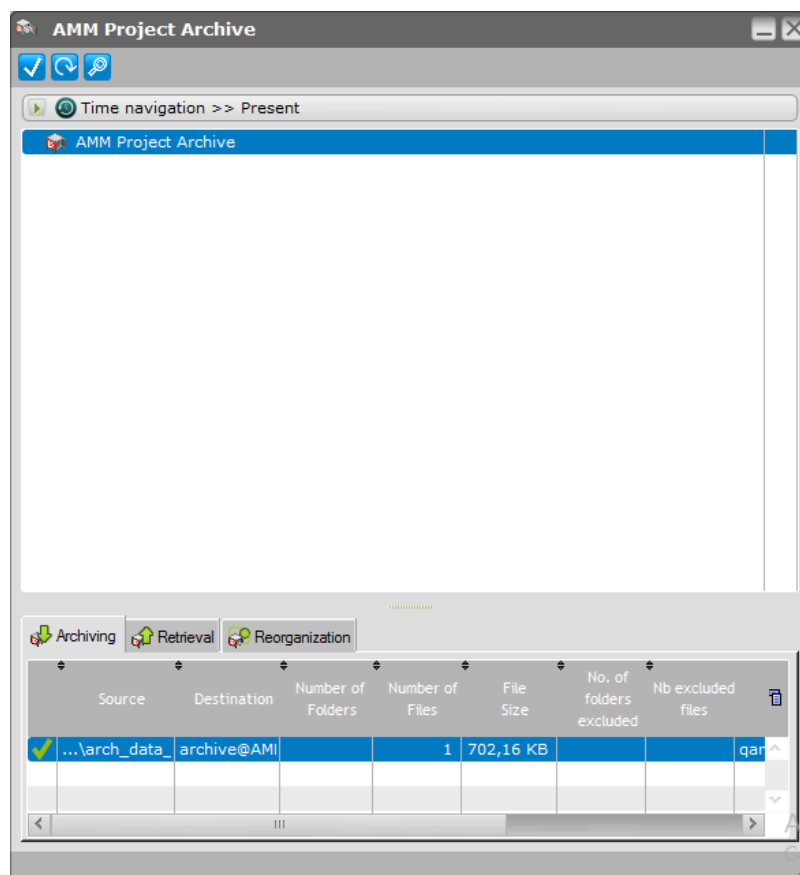


Figure 72: The folder opens in the table on the Archiving page

5. Click ☒. Miria creates the archiving job, which will run as soon as resources are available.
6. On the confirmation message that opens, click **OK**.

Monitoring a Job

You can follow the progress of your job and troubleshoot issues from the List of Jobs interface. In addition to the information it provides, the List of Jobs provides access to a range of other monitoring functions.

To monitor an archiving job in the List of Jobs interface

1. On the left pane of the Administration Console, click **Jobs**.
The **List of Jobs** window opens.
2. In the **Current** table, look for a job that shows as Archiving in the **Action** column.
Initially, the Job Status is In queue.
Once the job begins to run, the status updates to Running.
Finally, when the job completes, it is moved to the History table with a Job Status of Completed (Figure 73).

	Action	Status	Archive	Expected Volume / Volume	Platform / ADA Agent	Source	Submission Date	Date of Update	User
Current									
History									
19	Archiving	Completed	AMM Project Archive	4.96 MB 100.0 %	Dell-T110	Graphic Interface	1/6/2012	1/6/2012	root
19	Archiving	Completed	AMM Project Archive	4.96 MB 100.0 %	Dell-T110	Graphic Interface	1/6/2012		

Figure 73: Completed jobs in the History table

To view the events associated with a job

- > Right-click the line of the job in the Current or History section of the table and choose Events from the pop-up menu.

Events provide useful information on how the job ran and how you can filter and sort it on a full range of criteria.

If you see any errors during the archiving process, see the Administrator Documentation.

To view media associated with an archiving job

- > Right-click the line of the archiving sub-job in the Current or History section of the table and choose Media from the pop-up menu (Figure 74).

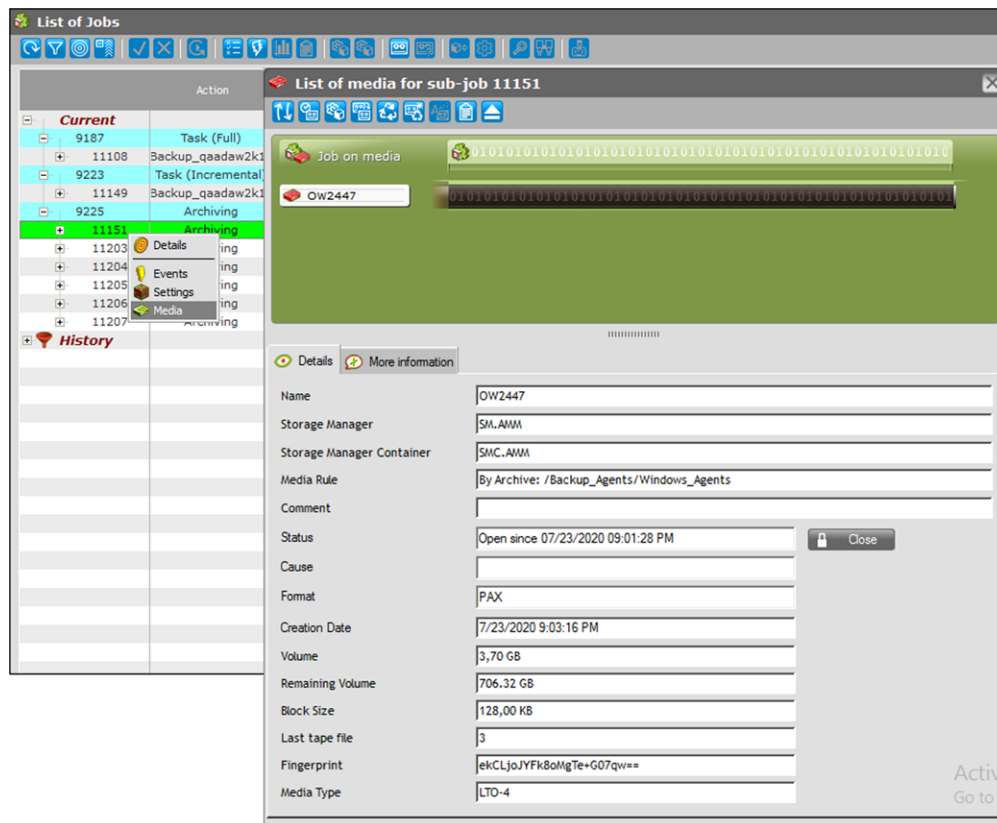


Figure 74: Media is displayed for a current sub-job

In addition to providing such information on the media used for the job as its barcode, status, data format, etc., the List of media interface includes buttons that enable you to act directly on the media (e.g., request media ejection).

To request media ejection from the library

- > In the icon bar, click the Request Ejection button. Depending on the configuration, the media is automatically ejected from the library, or requires the media administrator's manual intervention.

There are several other ways to view and monitor Media Manager media from Miria interfaces. For details, see the Administrator Documentation and the User Documentation.

Retrieving a File

Just as you used the Project Archive to archive data, you can use it to retrieve data. To do so, you can open the Project Archive and choose the data to be retrieved.

1. On the Administration Console, select **Storage > Project Archive**.
2. Right-click the **AMM Project Archive** project archive in the list in the center pane, and then choose **Open Archive**.

The **Project Archive** window opens and displays the contents of the archive ().

Note: If the Archive window remained open during archiving, refresh the display to view the newly archived files and select them for retrieval.

3. Expand the tree to navigate to the files to be retrieved.

4. To retrieve, right-click the file name in the table, and then choose **Retrieve**.
5. The **Retrieval Destination** dialog box opens; the Source field indicates the path of the file to retrieve:
6. Click the **Browse** button to the right of the Destination field to choose the path where you would like to save the retrieved data on the local machine where the Administration Console is running.
The **Browse for Folder** window opens.
7. Select the path and click **OK**.
The files you chose open in the Retrieval table (Figure 75).

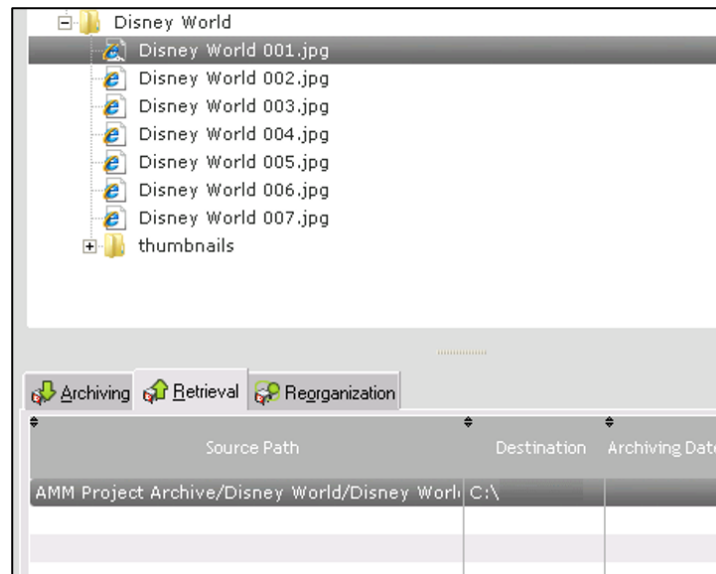




Figure 75: Selected file in the Retrieval table

8. On the **Project Archive Contents** window, click .
9. On the confirmation message that opens, click **Yes**.
Miria creates the retrieval job, which will run as soon as resources are available.
10. To close the **Project Archive Contents** window, click the [X] in the title bar.
11. To monitor the retrieval job, in the left pane of the Administrator Documentation, click **Jobs**.
The **List of Jobs** window opens.
12. In the Current table, in the **Action** column, look for **Retrieval**.
 - Initially, the Job Status is In queue.
Once the job begins to run, the status updates to Running.
Finally, when the job completes, it is moved to the History table with a Job Status of Completed.
 - As with archiving jobs, you can view the events associated with the retrieval job by right-clicking the job and choosing Events from the pop-up menu.
 - To view the media needed for the retrieval, right-click the retrieval sub-job and select List of Requested Media in the pop-up menu. If you have ejected a media that needs to be online for the retrieval to complete, the icon  can be displayed on the Sub-job of the running Retrieval Job. It signals that you must physically put the media back in the library.

See [Monitoring a Job](#) and the Administrator Documentation for details on viewing events and media from the List of Jobs.

13. To verify, check for the retrieved files in the destination folder you chose.



APPENDIX Migrating the Database from a Version prior to 3.10

Important: Make sure to close all the MaxDB consoles and tools before starting the database migration. Make sure to upgrade to version 3.8 when using MaxDB 7.7 with a Miria version < 3.4.

When upgrading from a Digital Archive lower than 3.10, you must migrate the internal ADA database & AMM database to the latest version. The migration procedure of the database comprises three steps:

1. Upgrading the Digital Archive to version 3.10 by running the setup program.
2. Migrating the database by running the `ada_service` command with `-db_migrate` argument.
3. Migrating the AMM database by running the AMM script.

Note: If your configuration includes a standby Digital Archive server, please contact Professional Services to help you perform the upgrade.

Migration prerequisites

- Ensure that the service is stopped on the server.
- When migrating the MaxDB database for a Windows or Linux version:
 - The migration is performed in place, so you do not need to have an extra disk space.
 - The database migration takes less than 10 minutes.

Upgrading Digital Archive

When running the 3.10 setup program, all binaries are copied to the Digital Archive server, including the data that is necessary to operate the new database version. However, the setup program does not migrate the data to the new database, neither does it start the services related to the new version of the MaxDB database.

At this point you can start Digital Archive 3.10, which will work with the previous database version. It can continue working this way, but two limitations

apply:

1. An automatic backup of the database cannot be performed.
2. The server cannot be updated to a new Service Pack or Release.

It is therefore recommended to perform the manual database migration to implement the updated version of the database.

Migrating the Digital Archive Database to the New Database Version

The data migration is performed manually by running the `ada_service` command with the `-db_migrate` argument. The migration is not performed if:

- The ADA service is running.

Or

- The MaxDB version is different from the version installed by the setup.

To migrate database data:

1. Stop the ADA service (Miria:Engine).
2. Run the `ada_service -db_migrate` command.
3. Start the ADA service (Miria:Engine).
4. Launch the Administration Console and verify that all your items (Archives, Storage Managers, Users) are still present in the database.

Migrating the Media Manager Database to the New Database Version

The data migration is performed manually by running database migration script.

To migrate database data:

1. Stop ADA service (Miria:Engine)
2. Run the script :
 - On Linux: `/Miria/AMM/bin/AMM_Migrate.sh`
 - On Windows: `C:\Miria\AMM\bin\AMM_Migrate.cmd`