AcuoStore Digital Asset Manager

Installation and Operations Guide

Release 6.0

Document Revision A

Last Updated: May 2013

Installation and Operations Guide

Revision A – April 2013

License Agreement

AcuoStore Digital Asset Manager is an Acuo Technologies licensed software product. Please refer to the separate *Acuo Technologies Software License Agreement* for complete licensing information.

Trademarks

All company and product names are trademarks or registered trademarks of their respective holders.

Corporate Headquarters
Acuo Technologies
Riverview Office Tower
8009 34th Avenue South
Suite 900
Bloomington, MN 55425 U.S.A.

952-905-3440
952-905-3441 (FAX)

World Wide Web Site
http://www.acuotech.com

Publication Date: May 1, 2013

Contents

List of Figures

Chapter 1 – Introduction

In this chapter:

- Purpose of this Installation and Operations Guide
- Who Should Read this Guide
- How to Use this Guide
- Related Documents and Reference Sources
- Conventions Used in this Guide
- Recommended Support Process

Purpose of this Installation and Operations Guide

Acuo Technologies prides itself on the customized assistance it provides to customers in support of the installation and implementation of new systems. This guide is to be used in conjunction with that process and serves as a reference for how to perform many routine, daily operational tasks – such as how to install databases, configure AcuoStore managed shares and applications, perform remote management, and handle system backup and recovery planning.

The guide describes all available AcuoStore features. However, certain features are individually licensed and may, therefore, not be part of your currently installed AcuoStore system. Please contact Acuo Technologies if you would like to add more capabilities to your current AcuoStore implementation.

Who Should Read this Guide

This guide is written primarily for a system administrator level person who may typically work with a database administrator charged with maintaining the Acuo Technologies server and applications. Much of what is involved with actually operating Acuo Technologies' products is installing and configuring them. So someone such as a system administrator or database administrator who is experienced using these types of products on a daily basis will best be able to perform the tasks described in this guide.

How to Use this Guide

If you are simply referring to this guide at some point after the initial installation and implementation of the product, you will probably not need to revisit material such as the Getting Started information. However, if you are new to Acuo Technologies' products, it is recommended that you read the Overview to get a better understanding of the general environment in which the products operate and the functions they perform. After that, refer to the other chapters of the guide for specific information on the tasks you need to perform.

The following topic summarizes by chapter the types of information this guide contains.

Contents of this Guide

Here is a summary of the information provided in this document:

- **Chapter 1 - Introduction:** This chapter provides an overview of the information that you will find in this document along with information about how to best use the document. In addition, it provides key information such as how to contact technical support.
- **Chapter 2 – AcuoStore Overview:** This chapter describes the overall environment in which the AcuoStore product works and provides valuable insight into how it can be used to advantage. In addition, it also summarizes the product's key functions.
- **Chapter 3 – Getting Started:** This chapter gives step-by-step procedures for installing AcuoStore, creating an MMC console, and performing AcuoStore database installation.
- **Chapter 4 – AcuoStore Configuration:** This chapter provides an AcuoStore configuration example that includes step-by-step instructions of how to build the sample configuration.
- **Chapter 5 – Remote Management:** This chapter provides information describing the various ways in which you can manage AcuoStore functionality from a remote site.
- **Chapter 6 – System Backup and Recovery:** This chapter covers system backup and recovery procedures and other procedures required to keep databases in sync and their contents protected.
- **Appendix A – Frequently Asked Questions:** This appendix includes a number of answers to frequently asked questions.
- **Appendix B - Troubleshooting:** This appendix describes available troubleshooting aids and the various steps you can take if you encounter problems using Acuo products.
- **Appendix C – AcuoStore Network Profile:** This can be used as a reference when planning or troubleshooting Anti-virus, firewall, VPN, load balancing or other network related technologies in conjunction with an AcuoStore deployment.
- **Glossary:** The glossary contains definitions of terms and acronyms used in Acuo Technologies' product environments.

Related Documents and Reference Sources

There are a number of very useful related documents and reference sources that you may want to review. These include the following:

- The *AcuoMed Image Manager Installation and Operations Guide* or, if you are using a client application other than AcuoMed, reference the documentation that comes with that product.
- The Windows Server Help System and the Microsoft SQL Server Help System, accessed by choosing Help from the Windows Start menu.

Conventions Used in this Guide

It is important to keep in mind a few basic conventions used for presenting information in this document. These conventions are summarized below.

Procedures

As much as possible, instructions for performing installation and operational tasks are presented by means of procedures. A procedure consists of several numbered steps to be performed in sequence. Procedure steps are numbered and may include additional explanatory information as is appropriate. Here is an example of how procedure steps appear in this manual:

1. Before beginning installation, review configuration recommendations.

   Chapter 3 – Getting Started, provides hardware, software, network, and offline storage configuration information.

2. Back up the target system before starting Setup.

   Make sure a full backup of the system and its registry is done before proceeding with installation.

Optional Procedure Steps

Certain steps in a procedure may not be required in all cases. Procedure steps that contain optional actions are indicated by the word (Optional) in parenthesis at the beginning of the procedure step, as shown in the example here:

1. (Optional) For maximum protection, make a second backup of your current data before beginning installation.

What Keys and Buttons Look Like

Specific keyboard keys that you are instructed to press appear in boldface type, as in the following example:

Press **Enter** to continue.

On-screen buttons that you are instructed to click appear in two ways:

- For labeled buttons, the button's label appears in boldface type, as in: Click **OK** to continue.
- For icon buttons, the icon appears in the text, as in: Click  to save your file.

Notes, Cautions, and Warnings

Notes provide additional explanatory information or special instructions that apply to the process you are currently doing. Notes can also contain tips and special instructions about things you need to do under certain conditions. Here is an example Note.

NOTE:	You should read all notes to be sure not to miss any important installation or operations information.

Caution messages call your attention to conditions or actions that may result in damage to hardware or software systems or that may jeopardize operational integrity or your data. An example caution looks like this:

Caution

Close Microsoft Windows before powering off your workstation. Powering down with Windows running may cause future operational problems in your Windows environment.

Warning messages alert you to conditions or actions that may result in personal injury to you or serious damage to your system, operational environment, or data. An example Warning looks like this:

Warning

It is possible to delete assets using the pop-up menu that is accessed by right-clicking an AcuoStore application. This will actually remove the digital assets from the system. Be careful **NOT** to select Delete Assets from the pop-up menu unless you intend to permanently remove the application's digital assets from the Acuo system.

Recommended Support Process

In order to appropriately track your support requests, during or after business hours, please use our online web portal located at www.acuotech.com/support.html. New cases can be created and tracked via this online support tool.

Other ways to contact Acuo Support

In the event that your web portal request is not being handled appropriately please feel free to contact us via email or phone:

- support-escalations@acuotech.com
- Calling 866-272-2286 (Acuo) will prompt callers to:
  - Press 1 for Software Support
  - Press 2 for Migration Support
  - Press 0 for all other inquiries

Chapter 2 – AcuoStore Overview

In this chapter:

- The AcuoStore Digital Asset Manager
- AcuoStore Architecture
- Storage Management Interface

The AcuoStore Digital Asset Manager

The AcuoStore Digital Asset Manager (or AcuoStore for short) is a general-purpose, digital asset management service that lets you store, track, and retrieve virtually any type of digital asset routed to an AcuoStore archive from a client application such as AcuoMed. Functioning like a digital vault for the client application, AcuoStore checks digital assets into and out of storage archives that have been configured to store digital assets. AcuoStore itself features an easy-to-use interface that allows an administrator to set up and manage secure, easily expandable storage archives on devices such as RAID 3 and RAID 5 disk arrays, tapes, and local servers, and several supported archiving devices.

As it is being currently implemented, AcuoStore is part of a medical image storage system that collects and distributes images from medical modalities such as CT scanners, ultrasound machines, and other image-based devices. In this context, subscribers (for example a medical professional, hospital, or clinic) have access to and use AcuoStore archives to store and retrieve medical-based images. However in all contexts, subscribers have a unique Subscriber ID that allows them to store the kind of digital assets that they use in archives to which they subscribe. By giving subscribers their own ID, AcuoStore can let multiple subscribers share an archive and, at the same time, assure that one subscriber cannot access the assets of another subscriber. As might be expected, depending on configuration constraints and usage needs, one subscriber may have access to multiple AcuoStore archives.

When it receives a digital asset from a subscriber, AcuoStore automatically assigns the asset a Globally Unique ID (GUID) and returns it to the subscriber. The GUID identifies the specific asset for future retrieval. When a subscriber wants to retrieve a digital asset, he or she simply enters their AcuoStore archive, submits the GUID associated with the desired asset, and AcuoStore makes the asset locally available.

For off line storage needs, a Content-Addressed Storage (CAS) or Fixed Content Storage (FCS) Device can be installed to receive and store image files from AcuoStore based on pre-configured parameters indicating how long files will remain in cache, and when the files will be written to the Archive Device. These parameters are configurable for each Application within AcuoStore. When the writing process to the Archive Device is complete, it returns a Clip ID which is stored in each files' metadata that tracks its contents in the Archive Device. AcuoStore uses the Clip ID to relocate the file in the Archive Device and makes the file locally available.

Figure 1 displays how the AcuoStore Digital Asset Manager serves as a digital vault between the client application and the physical storage space.

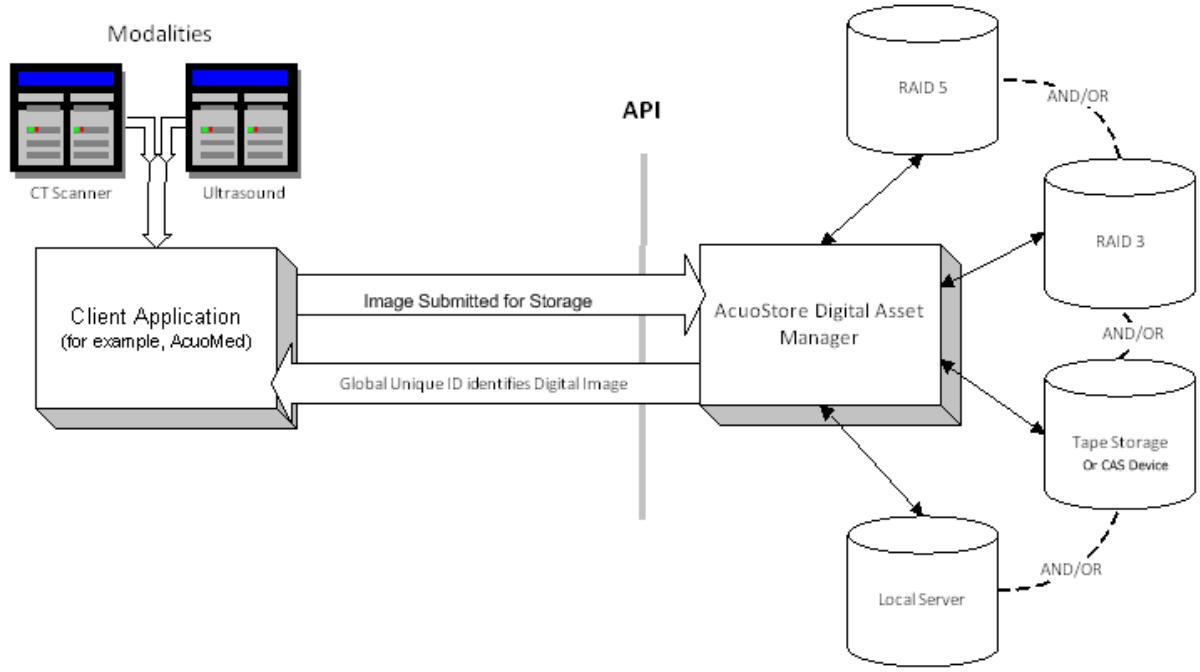


Figure 1: AcuoStore as the digital vault

Who Needs AcuoStore?

Organizations that generate a large amount of digital data that must be stored, searched, and retrieved can use AcuoStore to their advantage. In a medical context, such organizations include hospitals with clinics spread out over a geographic area. These organizations can take advantage of AcuoStore's push-based technology to send images to other servers where medical professionals who need to examine the images are located.

Some other environments and organizations that may make use of AcuoStore include law firms, manufacturers, or retail stores that store and retrieve digital images on a regular basis. AcuoStore, through its easily expandable, modular architecture, makes it practical to build a system that can grow with an organization's needs. The following topic, *Basic Usage Scenarios*, describes several scenarios which illustrate that AcuoStore is designed to handle all asset volume levels. The strength of AcuoStore is in its ability to provide a reasonably simple way to set up, organize and then channel digital assets into a safe, yet easily accessible storage compartment using readily accessible Windows Server technology.

Basic Usage Scenarios

The following three basic usage scenarios describe a tiered system of storing digital assets based on how long ago they were generated or last accessed. Using a tiered approach, the system seeks to overcome the limitation that not all of your digital assets can be kept online where they are immediately accessible. Generally, assets stored in the system more recently are usually available in less time while assets stored in the system longer ago will generally take longer to retrieve.

There are three basic usage scenarios:

- Online Storage
- Nearline Storage
- Offline Storage

Online Storage

Online storage is characterized by quick access and is usually implemented via a RAID device on a local server. Acuo Technologies recommends sizing online storage to hold digital assets received over the last one year period. Refer to *Appendix C – Storage Analysis* in the *AcuoMed Image Manager Installation and Operations Guide* for assistance with sizing storage devices.

When using a CAS Device, Online means the data only resides on the local cache, and no copy exists on the CAS Device (if configured).

Nearline Storage

Nearline storage is characterized by the use of tapes in a tape library that can be mounted when they are needed with the use of robotics such as a jukebox. Accessing these tapes does not require manual intervention. When a tape is called, the jukebox picks the appropriate tape and puts it into a drive that can be accessed online. Acuo Technologies recommends sizing nearline storage to hold digital assets for up to a 5-year period, depending on your requirements. Refer to *Appendix C – Storage Analysis* in the *AcuoMed Image Manager Installation and Operations Guide* for assistance with sizing storage devices.

When using a CAS Device, Nearline data is on the local cache and a copy also exists on the CAS Device.

Offline Storage

Offline storage refers to shelf storage of tapes. If information in offline storage is required, an operator must retrieve and mount the appropriate tape(s) in a robotic device such as a jukebox. Tapes usually have human-readable barcodes on them so that they can be easily identified. Offline storage provides an almost unlimited amount of long-term storage space. However, care should be taken to store tapes properly. Store tapes in a temperature and humidity controlled environment where tapes are not in direct sunlight or subjected to any magnetic interference.

When using a CAS Device, Offline is data that has been deleted/purged from the local cache and only remains on the CAS Device.

Password-Level Security

Password-level security refers to using Login/Password information to control access to the AcuoStore database for the AcuoStore application itself. The client application, such as AcuoMed, and AcuoStore applications are the only services that should be allowed to access the AcuoStore database.

As a person using AcuoStore, you will not be asked to supply this Login/Password information at any time during day-to-day operation of AcuoStore. However, there may be cases where you need to change the

Login/Password information – for example, if your SQL Server administrator requires that passwords be changed every 30 days.

If your login or password information for SQL Server changes (by an administrator for example), you will need to change the login and/or password for AcuoStore in order for AcuoStore to continue to have access to the AcuoStore database. This change is made by right-clicking on the **AcuoStore Server** node in the MMC console tree and selecting **Change Database Connection** from the pop-up menu. This selection displays the Database Connection Parameters dialog (Figure 2). You then change the Login and/or Password parameters as required to match the new SQL Server Login/Password setup.

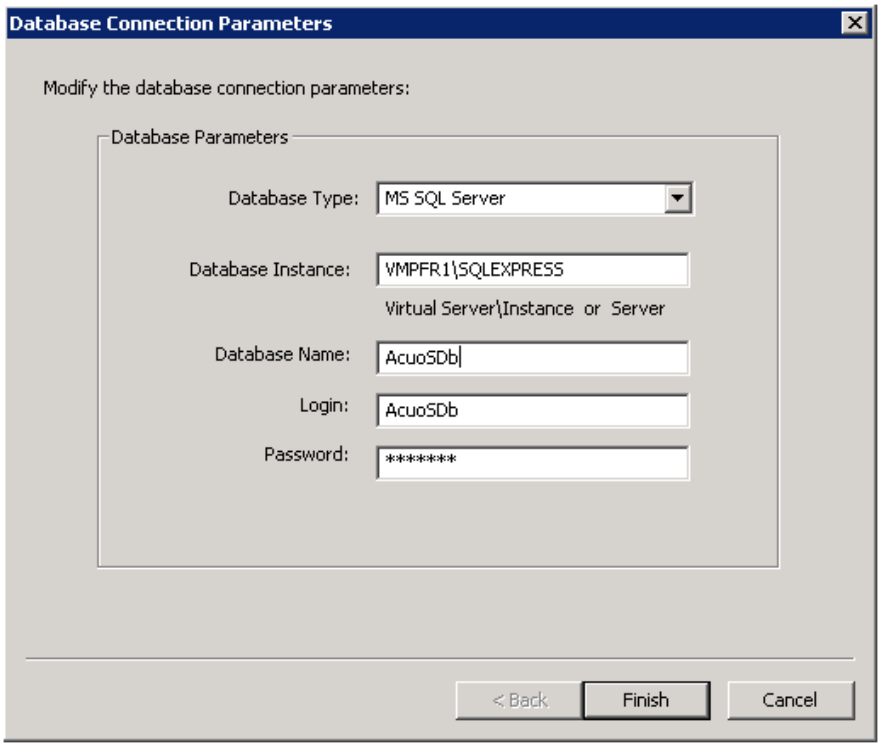


Figure 2: Database Connection Parameters – MS SQL Server

AcuoStore password-level security works in conjunction with standard Microsoft SQL Server security to ensure that only users with the proper system privileges can access the AcuoStore database. If you need additional information, contact the SQL Server administrator at your site or refer to the appropriate Microsoft SQL Server documentation.

Configuration Security – Microsoft Management Console

Configuration security refers to an administrator's control over the process of building an MMC console application and using this application to configure the AcuoStore service. An administrator can reserve these privileges for himself or can assign them to other users. An administrator can also build an MMC console, send it to another user, and then give that user the privilege to configure the AcuoStore service via that MMC console.

AcuoStore's configuration security is integrated with Windows logon security for MMC console applications. Through this integration, AcuoStore's configuration security allows an administrator to build toolboxes of management applications and assign Windows login and password level security to those console applications. Therefore, AcuoStore's configuration security runs within MMC security and observes all the controls and capabilities of MMC security. In addition, AcuoStore's configuration security will leverage any future capabilities that Microsoft may add to MMC security.

AcuoStore Architecture

By linking a manageably small number of products and confining AcuoStore to a straightforward set of configuration options, AcuoStore provides a simple, efficient way to securely manage digital assets. AcuoStore itself functions due to the configuration of just two primary components: managed shares and applications. These two components, once configured, serve as the key elements within AcuoStore that are responsible for carrying and directing digital asset traffic between the client application and the storage devices. Managed shares and applications are described in the following topics.

Figure 3 shows the AcuoStore architecture.

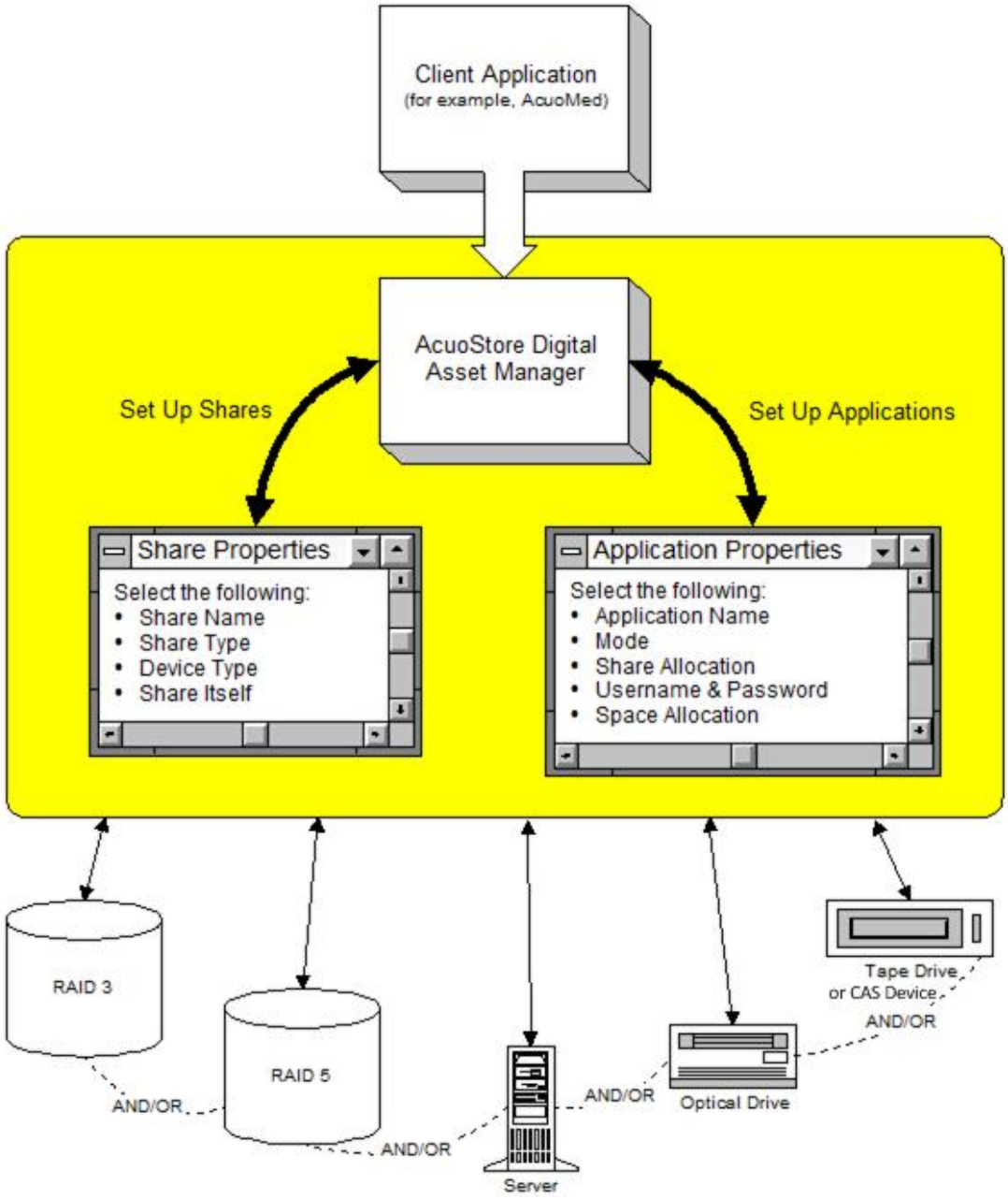


Figure 3: AcuoStore architecture

Managed Shares

A managed share is a logical mapping to a physical storage space. Configured using AcuoStore, managed shares function like conduits through which digital assets flow to and from specific storage devices such as RAID disk arrays, servers, optical drives, or other storage media. In contrast to applications that basically use shares to control traffic, managed shares function merely as the road on which the traffic flows.

You can configure AcuoStore to use virtually any type of conventional storage device that can be shared as an NTFS File System. Figure 4 illustrates these concepts.

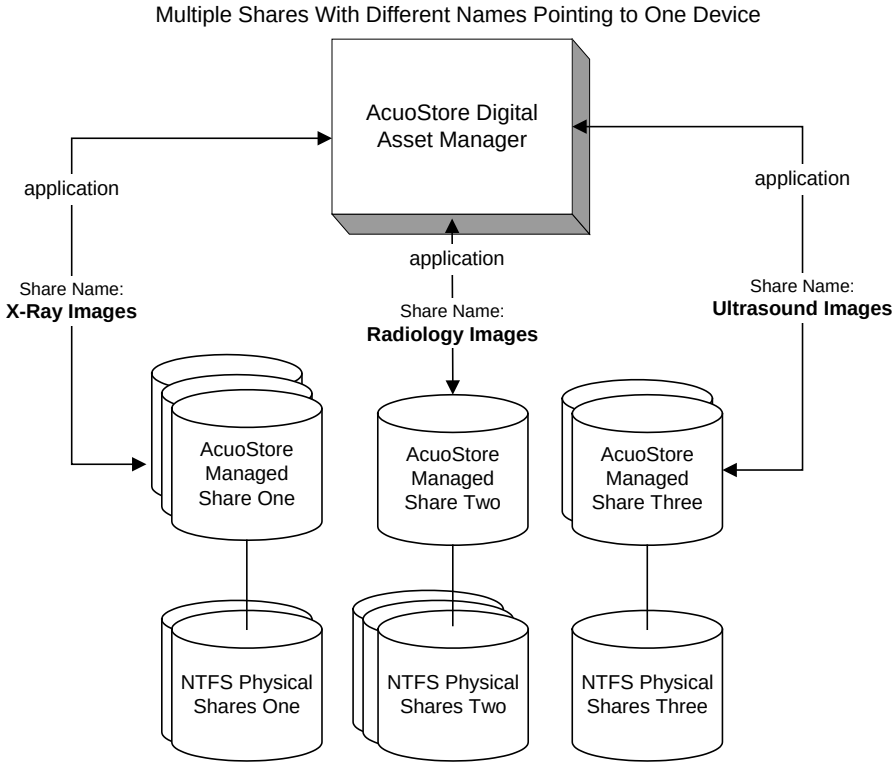


Figure 4: Managed share variations

As shown in Figure 4, note that AcuoStore Managed Shares are logical shares managing the data within NTFS Physical Shares. This type of NTFS Physical Share can extend the capacity of the Managed Share almost indefinitely and without the need to alert subscribers. From the subscriber's perspective they use the AcuoStore share *Radiology Images*. Thus from an administrative standpoint if you need to add storage space, once a managed share is set up all you have to do is logically attach a new storage device to your original managed share or add storage to an existing NTFS share.

NOTE: In Windows users must manually set the permission on each folder shared. Right-click on the folder to share → select properties → click on tab for sharing → select three Acuo Users (Acuo Administrators, Acuo Power Users and Acuo Users) and apply full permissions to Acuo Administrators, full permission to Acuo Power Users and read only permissions to Acuo Users. Do the same thing within the Security tab of the share folder.

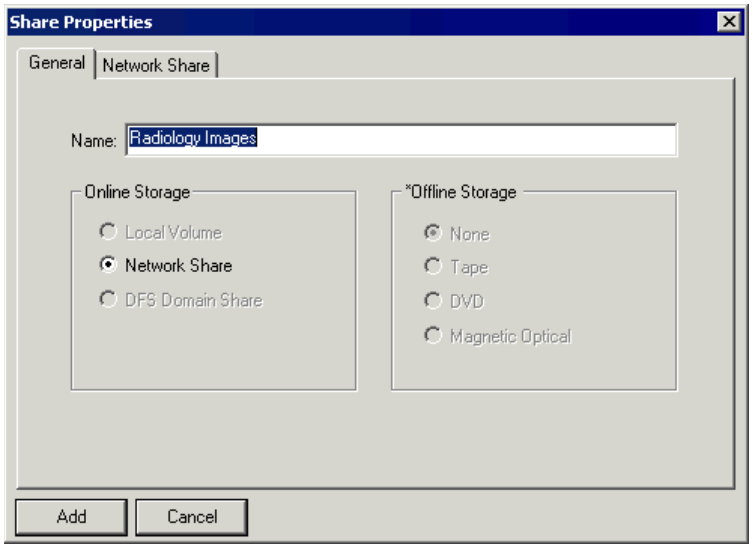
Managed Share Configuration Options

Managed share configuration options allow the administrator to set up shares and tailor them to conform to the client's particular hardware constraints. When setting up a managed share, you are given the following configuration options:

- Name the Share
- Select the Online Storage Type (Managed Share)
- Attach to the online storage type (Managed Share)

Name the Share

It is a good idea to give shares a name that means something to those who will be using the share. If AcuoStore is being implemented in a medical environment, then a name such as *Radiology Images* may represent a suitable example.



Select the Online Storage Type

There are three kinds of online storage types from which to choose:

- Physical Share (Local Volume)
- Network Share
- DFS Domain Share

Logical Share (Network Share)

A Logical share is the recommended share type. When a logical share is set up, being a logical share, it is actually considered a namespace. Since the share is to a namespace, it means that you may attach an almost unlimited number of physical devices to a namespace thus extending almost indefinitely the amount of storage space the namespace may represent. See the *Glossary* on page 95 for a more complete definition of the term namespace.

From a performance standpoint, a logical share, which is usually set up over a network, is generally slower than a physical share that is located on the same volume as the AcuoStore installation. However, this limitation is usually outweighed by the benefit of being able to easily expand the amount of physical storage space by adding more logical shares.

Physical Share (Local Volume)

A physical share is limited by how much space is actually available on the physical device. However, this limitation is offset to some extent by the increase in speed inherent with a local volume and the fact that certain local devices, for example a RAID 5 disk array, hold large amounts of digital information.

DFS Domain Share

A Distributed File System (DFS) is a file system that allows access to files from multiple hosts sharing via a network. This makes it possible for multiple users on multiple machines to share files and storage resources.

Attach to the online storage type – Network Share

Figure 5 shows the Share Properties dialog box for adding a Managed Share (Network Share) from within the AcuoStore GUI. To locate a share on a different device, you must first browse to that device. The local Server Name will otherwise appear in the Server Name field. To make an attachment, click the drop-down arrow on the dialog box that displays, navigate to the share to which you want to attach, and click **Add**.

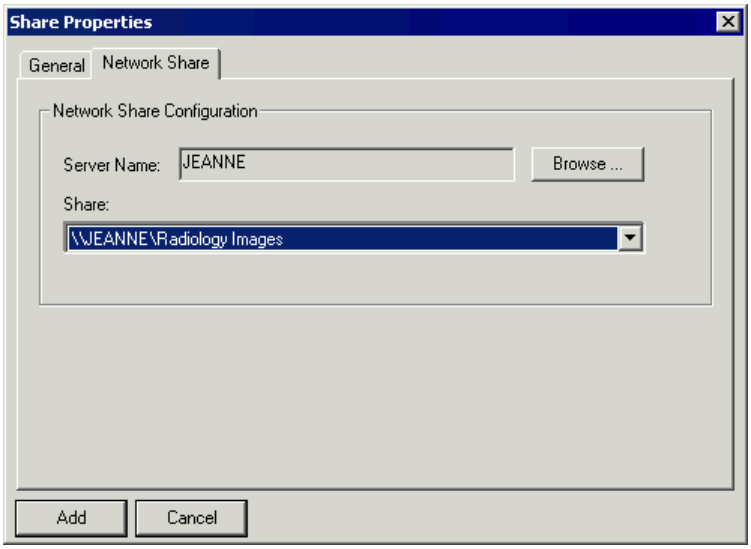
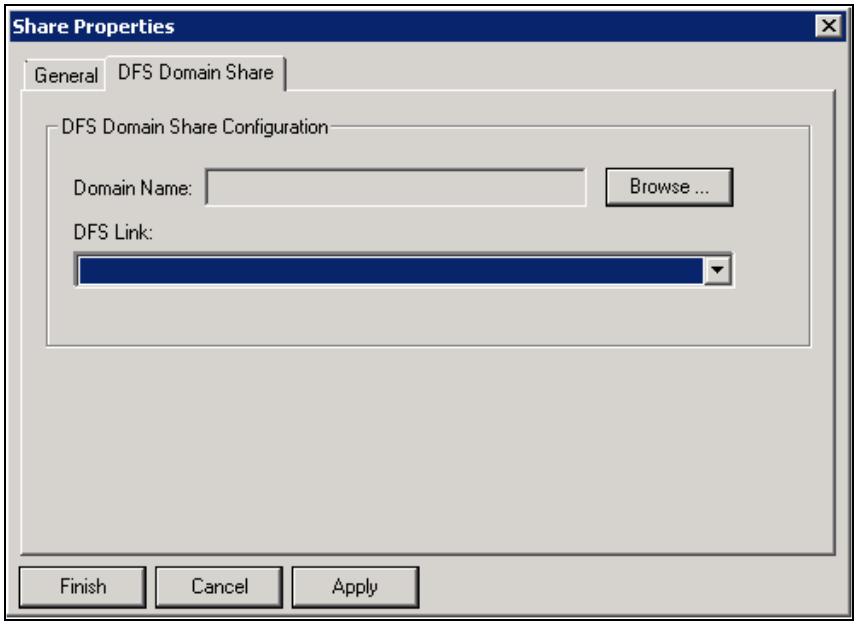


Figure 5: Network Share dialog box

Attach to the online storage type – DFS Domain Share

To create a Managed Share using a DFS Domain Share, click on the DFS Domain Share Tab, enter or browse to the appropriate Domain Name, and select one of the available DFS Links.



Applications

Once you configure their set of simple, straightforward options, applications let you control which subscribers have access to a managed share and how much space the subscriber can use on it. Like a digital safety deposit box, applications let authorized users into and out of storage devices in which a subscriber's digital assets are stored.

Applications provide the point at which the client application, for example AcuoMed, makes contact with AcuoStore. In practice, this means that via a client application, subscribers interface to an application and the application then either grants or denies the subscriber access to the managed share that houses their digital assets. When provided with the appropriate API calls, virtually any type of client (such as AcuoMed) can link to an application created using AcuoStore.

Finally, two or more managed shares can be allocated to one application to extend storage needs for that application. For example, say you have a current managed share that no longer has space available to store new images, so a new physical share and managed share must be created to extend your storage needs. Once the managed share is configured, all that is needed is to update the associated application, de-allocate the old managed share and allocate the new managed share. There are no changes made to the subscriber or AcuoMed User's point of view, and you can add storage as you need it.

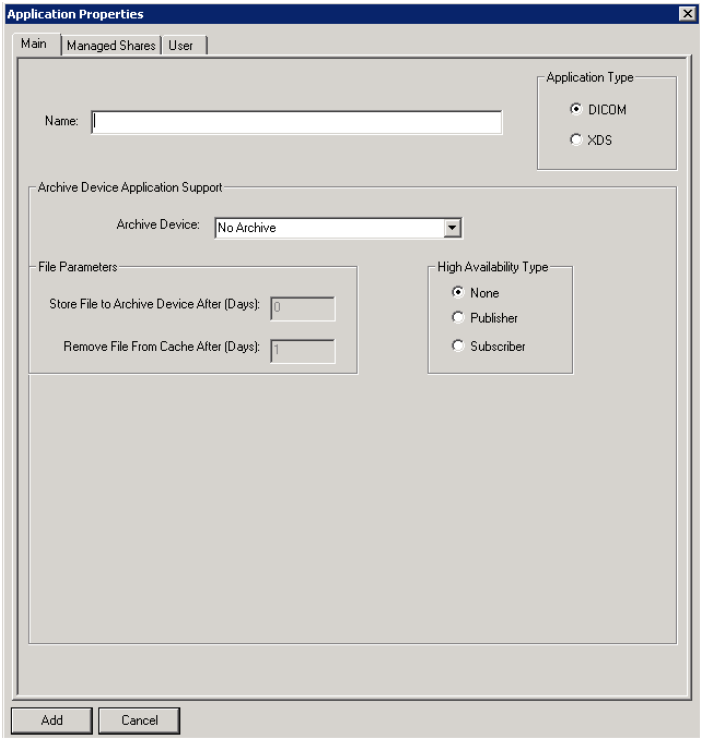
Application Configuration Options

Application configuration options allow the administrator to allocate specified amounts of storage space to particular subscribers and utilize the managed shares that have already been set up. When setting up an application, you are given the following configuration options:

- Name the Application
- Select Archive Device (Optional)
- Select Application Type (DICOM or XDS)
- Select High Availability Type (if applicable)
- Select an Active Share
- Select a User Name and Password
- Allocate Disk Space

Name the Application

It is a good idea to give applications a name that means something to those who will be using the application. If AcuoStore is being implemented in a medical environment or in a particular city, then a name such as *Rochester Images* may represent a suitable example.



Select Archive Device (Optional)

If an Archive Device is connected, select the device from the Archive Device dropdown menu. If the Archive Device is not connected to AcuoStore, this section will be grayed out. See the following section labeled "*Configuring an Archive Device*" for more information.

Select Application Type

Applications can be created for both DICOM and XDS implementations. The type is specified in the Application Type section.

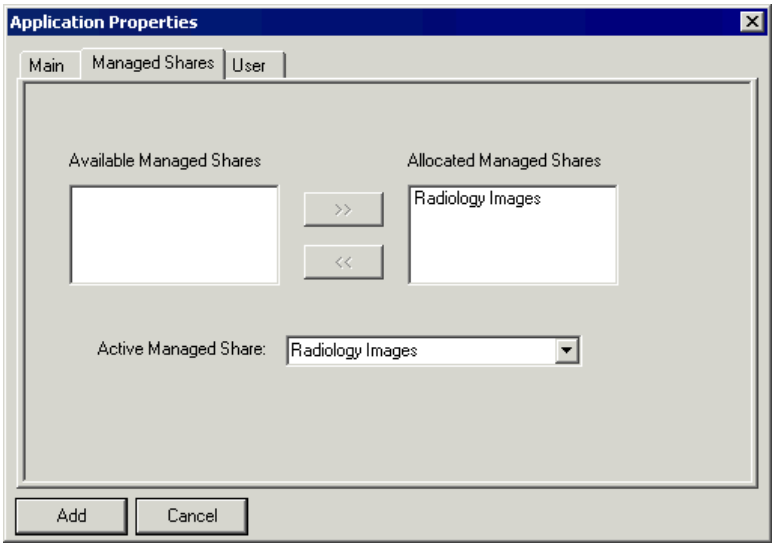
Select High Availability Type (if applicable)

Specify whether or not the application will use High Availability, and if so, what role the application will server (e.g., Publisher/Subscriber).

Select an Active Share

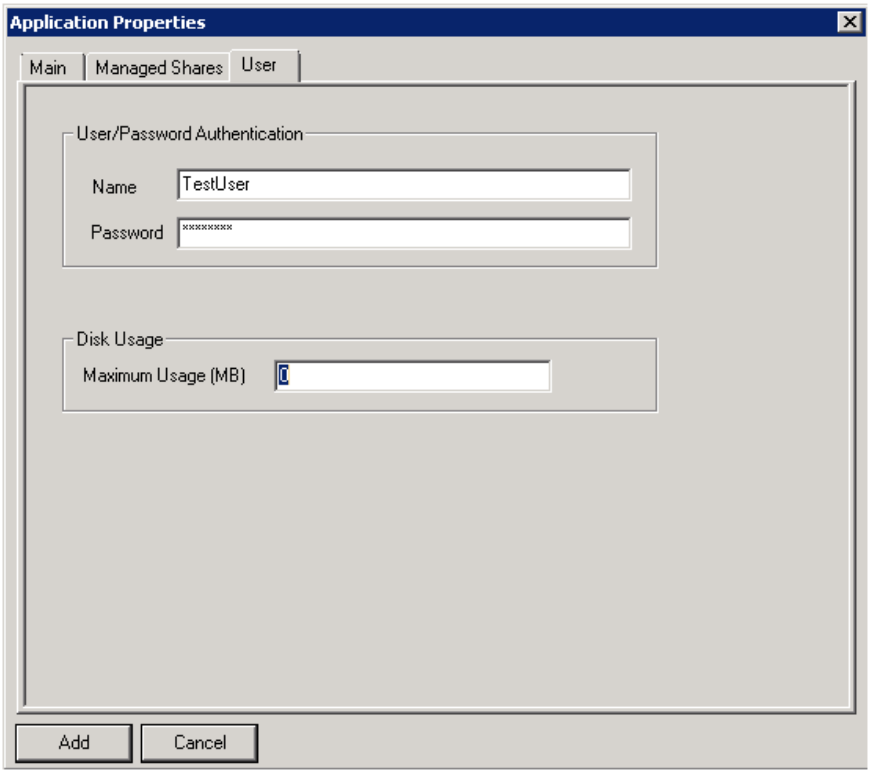
This option lets you select an active share from those that are available. To do this, on the Application Properties dialog box, click the **Managed Shares** tab, highlight an available share, and then click the right-arrow to move the share into the Allocated Shares window. The allocated share automatically becomes the Active Managed Share.

To deactivate a share, highlight an allocated share, and then click the left-arrow to move the share into the Available Shares window. If there are no other allocated shares, the Active Share field becomes blank. Otherwise, the next allocated share in line moves up and becomes the active share. Deactivating a share is not recommended if images are already stored and reside in that managed share.



Select a User Name and Password

This option lets you select a user name and password for each user that you want to access the active share you selected. To do this, on the Application Properties dialog box, click the **User** tab, and enter an appropriate user name and password.



To access the digital assets associated with the active share you selected, the user will need to enter the user name and password that you specified.

Allocate Disk Space

This option lets you select the amount of space you want to make available to the user on the active share that you selected. To do this, in the Application Properties dialog, click the **User** tab, and enter an appropriate amount of Disk Usage space in the Maximum Usage field (for example, 10 gigabytes). Entering 0 in the Maximum Usage field allocates unlimited disk space.

Click the **Finish** button to complete configuring the application and to select all your options.

Storage Management Interface

Storage management interface refers to the type of interface that must be in place to support, and in some cases enhance, AcuoStore functions.

There is one key interface:

- NTFS Interface

NTFS Interface

The NT File System (NTFS) is a file system that is available with Windows Server 2008 and later. This is the recommended file system, over FAT and FAT32, for AcuoStore applications due to the fact that it supports other needed features such as Distributed File System (DFS), Remote Storage Services (RSS), and file compression. An additional feature with NTFS is that it provides security levels that allow you to lock down file system access so that only users with administrator authorization can log on and look at the system's assets. Also, spanning volumes are only allowed in NTFS. Be sure that RAIDs are initialized as Dynamic Disks, if your implementation requires support for volume spanning. Dynamic disks are not supported in a clustered configuration, basic disks are required.

Chapter 3 – Getting Started

In this chapter:

- Recommended Configurations
- Pre-requisite Installation
- Host Server Setup
- AcuoStore Installation
- MMC Console Creation
- Database Installation
- Changing a Database Connection

Recommended Configurations

IMPORTANT: Prior to installing AcuoStore, ensure that your hardware, software and network components meet or exceed the recommended configuration levels detailed in the *AcuoMed Image Manager Installation and Operations Guide*. Even if you are building an AcuoStore implementation with a client application other than AcuoMed, the recommended components that are described in the AcuoMed manual will prove very useful in terms of ensuring your implementation's overall success.

AcuoStore Installation

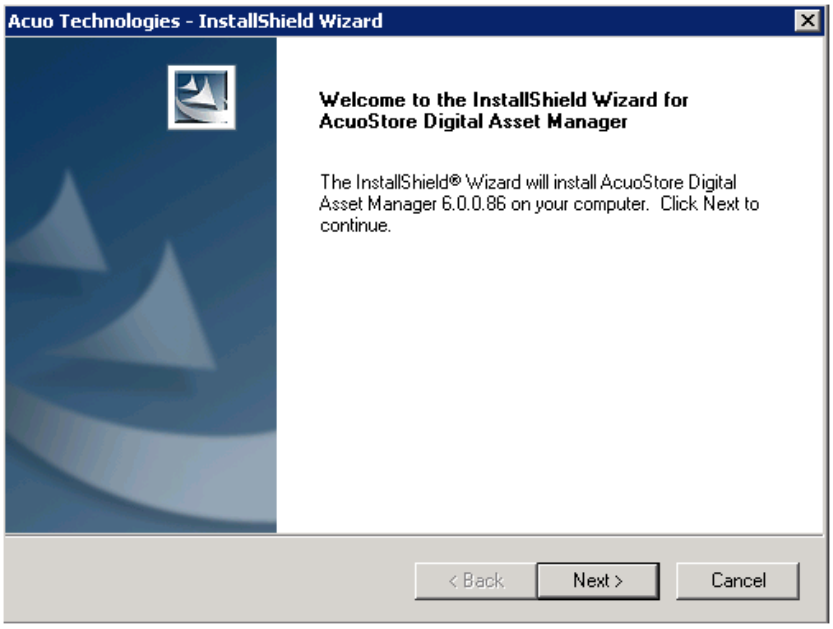
AcuoStore installation **must** be done before the client application installation (such as AcuoMed). Refer to the *AcuoMed Image Manager Installation and Operations Guide* for the AcuoMed installation procedure. For an overview of AcuoStore setup and configuration refer to *The AcuoStore Digital Asset* Manager on page 11.

Follow these steps to install AcuoStore.

1. Install Prerequisites.
2. Install Host Server Setup. (both x64 and x86)
3. Start the AcuoStore InstallShield Wizard.
    - Access the Acuo Installation software.
    - Expand the folder structure as follows:

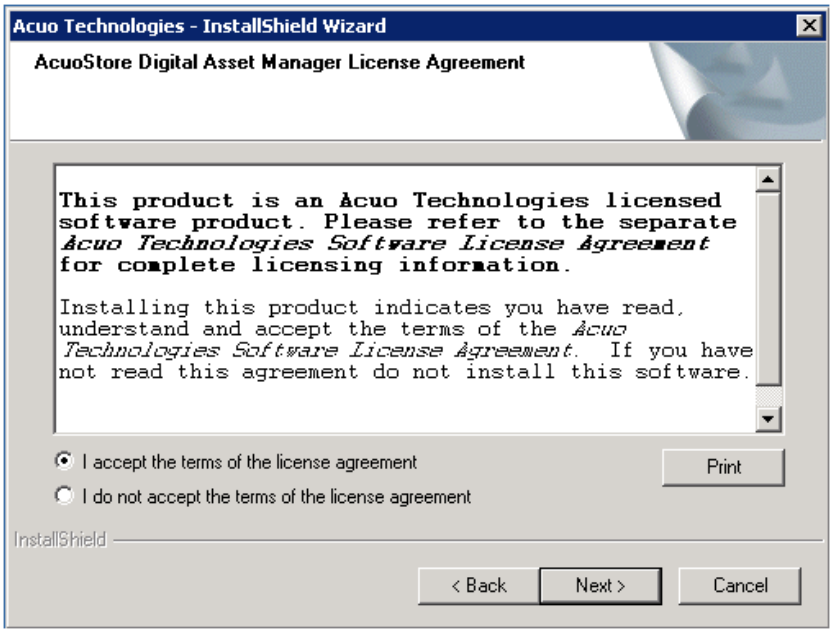
      AcuoStore Digital Asset Manager [Release # Build #]→AcuoStore Digital Asset Manager [Release # Build # Service Pack #]→DiskImages→DISK1
    - Locate and double-click the file **Setup.exe**.

The InstallShield Wizard Welcome screen displays.

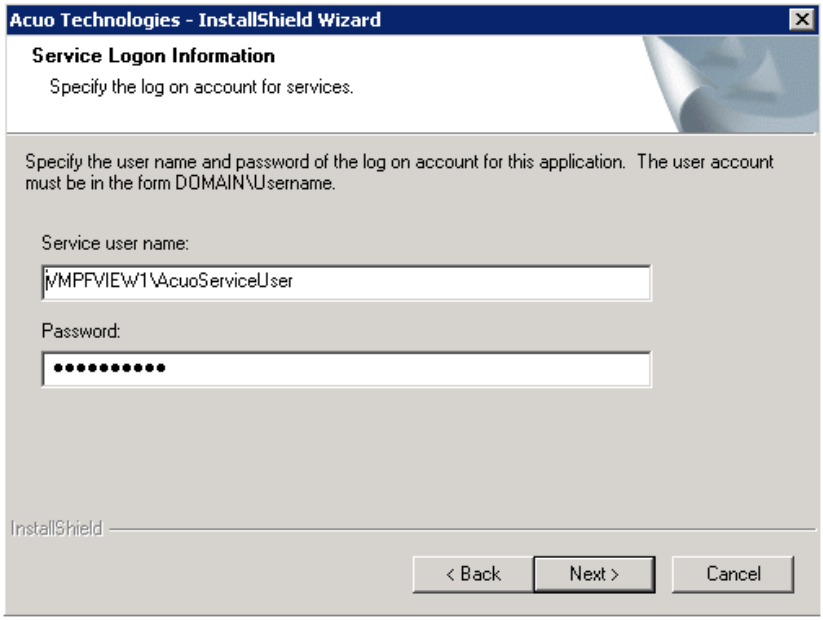


4. Click **Next** to begin the installation.

   The license agreement displays.

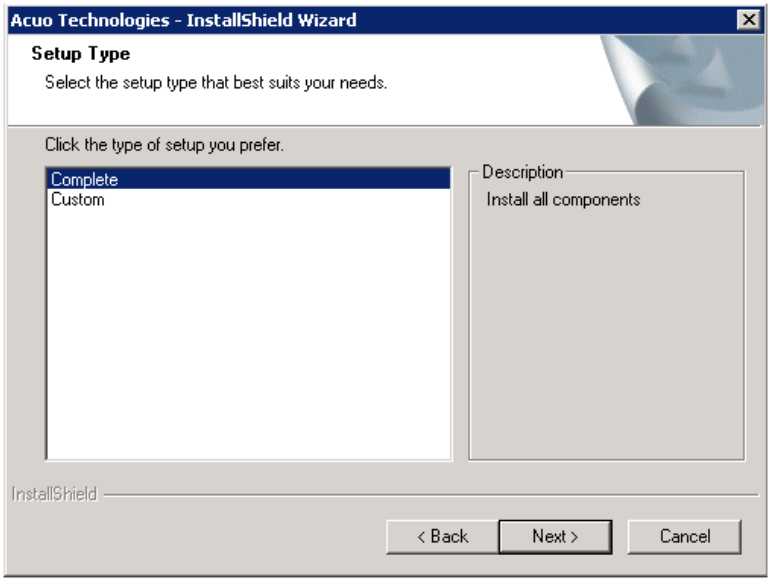


5. After reviewing the License Agreement, if you accept it, click **Next** to continue.



6. Type the desired Service User Name and password. Click **Next** to continue.

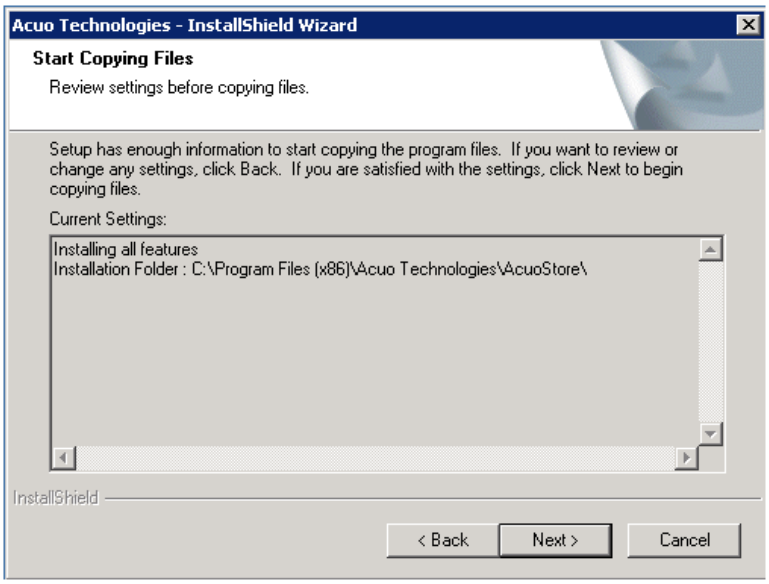
   The Setup Type screen displays.



7. To install all program features, click **Complete** and then click **Next** to continue (go to Step 11). Or to choose program features and install location, select **Custom** and then click **Next** to continue (go to Step 6).

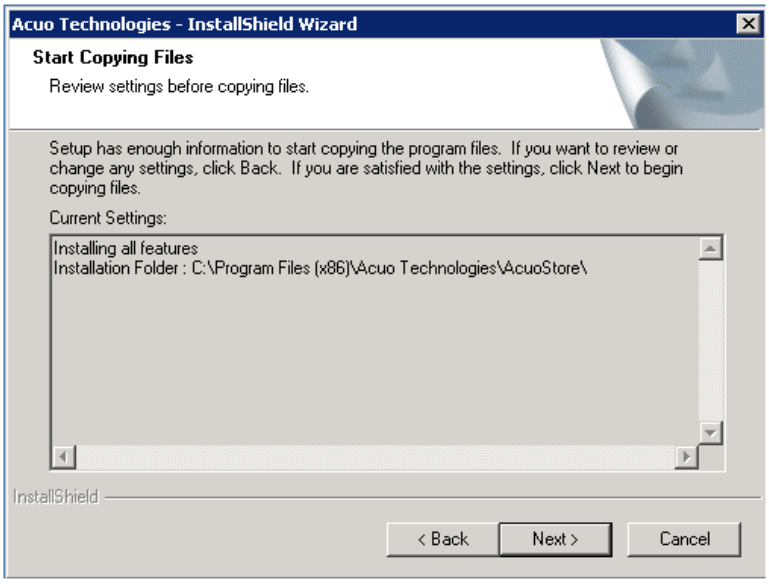
8. (Optional – for Custom Setup) – If you chose **Custom**, and select the **Browse** button you can modify the **Installation** location.

   You might want to do this, for example, if there is limited space available for the default install location.



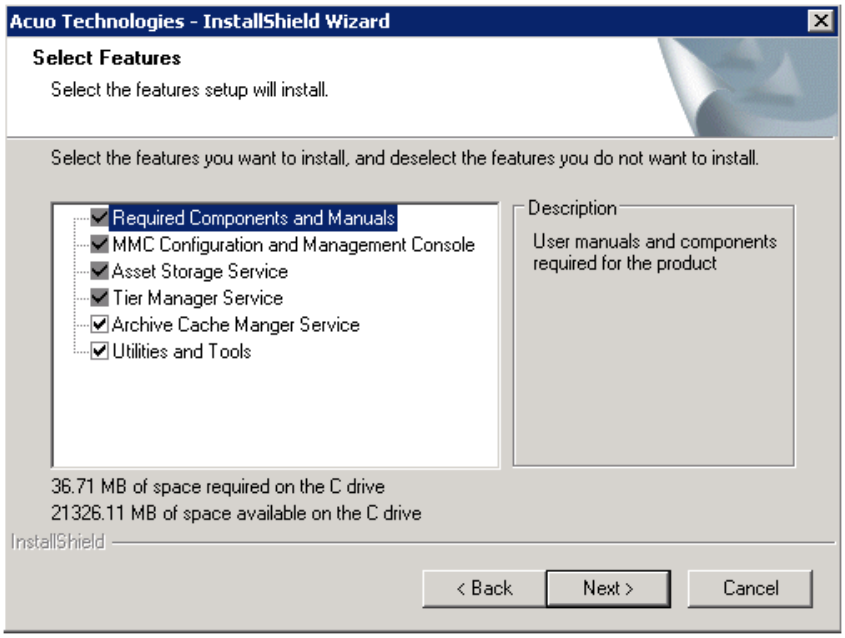
Should you want to install the software on a drive other than the C drive, click Back and choose Custom as noted in number 9 below. When changing the **Destination Folder** location, be sure to keep the AcuoStore installation on the AcuoStore Server system drive (that is, do not install AcuoStore on the drive where images will be stored).

9. (Optional – for Custom Setup) Click the Browse button to install the software in a different location on the system.



Browse for the new Destination Folder and then click NEXT.

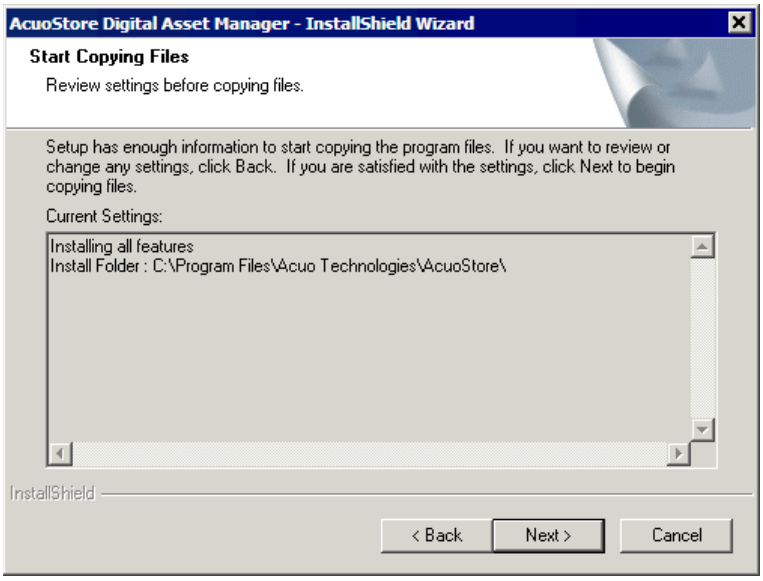
10. (Optional – for Custom Setup) Click one or more icons in the list to change how features will be installed (as shown in the sample below). The disk space requirement is noted as features are selected/deselected. Click **Next** to continue.



The features that can be configured by clicking the icons in the Custom Setup list have the following basic functionality:

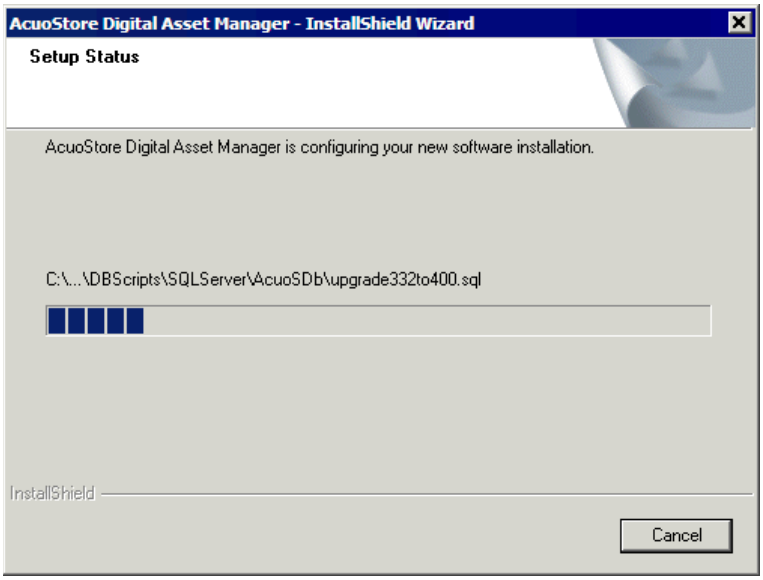
- Manuals and Required Components
- MMC Configuration and Management Console – the Microsoft Management Console components required to setup and operate AcuoStore and which provides remote management capabilities.
- Asset Storage Service – the AcuoStore product which is installed as an MMC snap-in.
- Tier Manager Service - The service is responsible for orchestrating the writing of assets to offline storage devices. (excluding EMC Centera devices)
- Archive Cache Manager Service – This service is responsible for managing the archive cache.
- AcuoStore Utilities - an AcuoStore program group that resides on the Windows desktop and provides quick access to a number of useful functions.

11. Before installing, you can review any of your installation selections and can change your selections by clicking **Back** to return to previous screens.

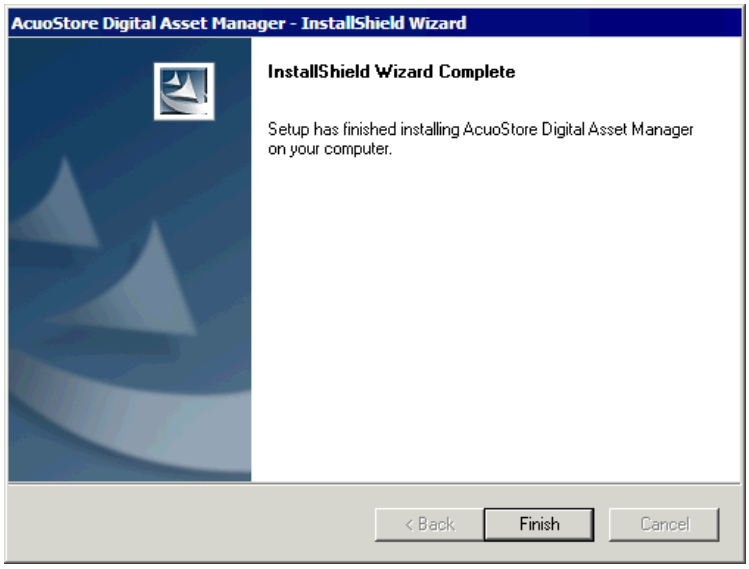


When you are ready to install the program, click **Next** to continue.

12. You can monitor the installation progress during the install process (as shown below).



13. When installation is finished, the InstallShield Wizard Complete screen displays.



Click **Finish** to exit the wizard.

Acuo Technologies Program Group

AcuoStore installation adds an Acuo Technologies folder to the Windows desktop. Double-clicking this folder icon launches the Acuo Technologies screen which provides quick access to useful Acuo and AcuoStore program functions.

The Acuo utilities are used for performing Acuo-wide program functions. Notice that there is a separate folder of AcuoStore Utilities. For information about the AcuoStore-specific utilities, see the next topic

AcuoStore Utilities

The AcuoStore utilities provide quick access to a number of useful AcuoStore-specific program functions.

To access these utilities, double-clicking the **Acuo Technologies** folder icon on the Windows desktop, and within the Acuo Technologies utilities screen, double-click the **AcuoStore Utilities** folder.

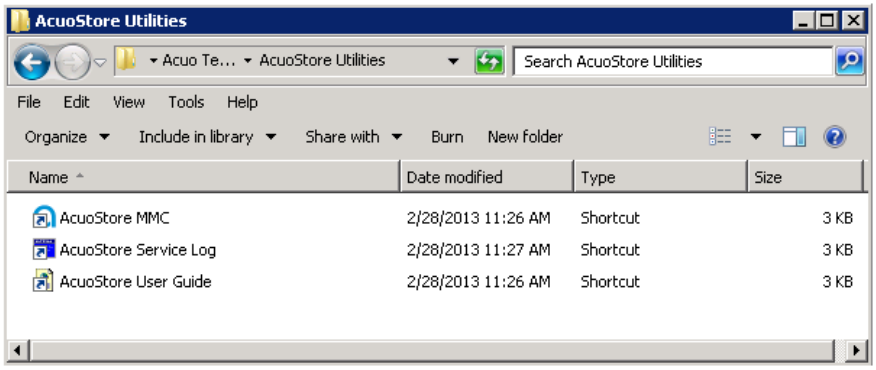


Figure 6: AcuoStore Utilities

The AcuoStore utilities perform the following functions:

- **AcuoStore MMC SnapIn** – creates a new MMC console that includes the AcuoStore Digital Asset Manager snap-in. If there is current AcuoStore configuration data on the server, this AcuoStore configuration will display in the new MMC console.
- **AcuoStore Service Log -** monitors the AcuoStore Interface Activity.
- **AcuoStore User Guide** – opens an electronic copy of the AcuoStore User Guide.

MMC Console Creation

MMC, which stands for Microsoft Management Console, is a framework for hosting administrative tools called consoles within Windows environment. MMC provides the tools and commands that you need to build new consoles. A console is an administrative structure that can contain tools, folders, web pages, and other administrative items. You can set up different consoles to manage different parts of your AcuoMed/AcuoStore network (for example, a local console and a remote console). Consoles are hosted within MMC.

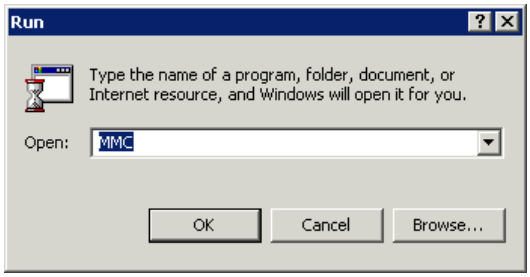
You can set up multiple consoles for different purposes and restrict their use by means of Windows security features. Using different consoles to manage different parts of your network is a good example of a case when you might want to set up more than one console. You can set up one console for local administration plus one or more additional consoles for remote administration.

Since you will operate AcuoMed and AcuoStore from an MMC console, you must create at least one console to which you will add the AcuoMed and/or AcuoStore service. It is also fine to add them to an existing console, if you prefer.

NOTE: A default AcuoStore console (AcuoStore.msc) ships with the AcuoStore product. You can either customize the AcuoStore.msc console, or you can use the procedure below to create a totally new console. Keep in mind that if you use the shipped .msc file, any setting changes made to that file will be lost upon reinstallation of the software.

Follow these steps to create an Acuo console.

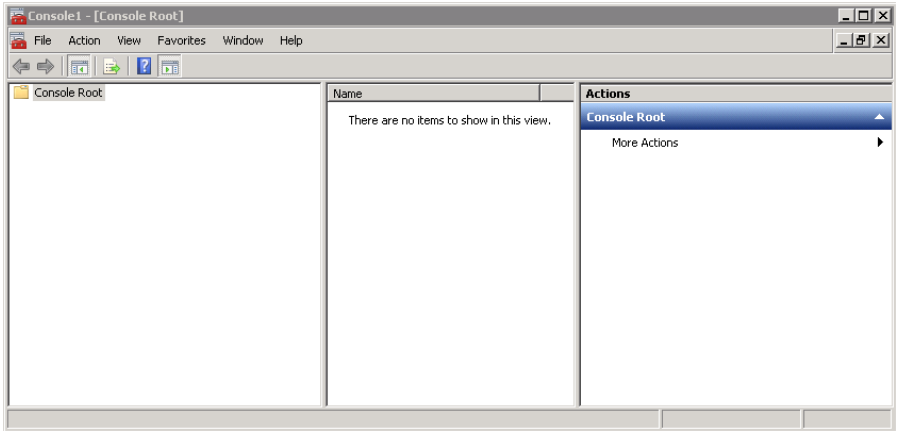
1. Click the Windows **Start** menu and then click **Run**.



2. In the Run dialog, type MMC (as shown above) and click **OK**.

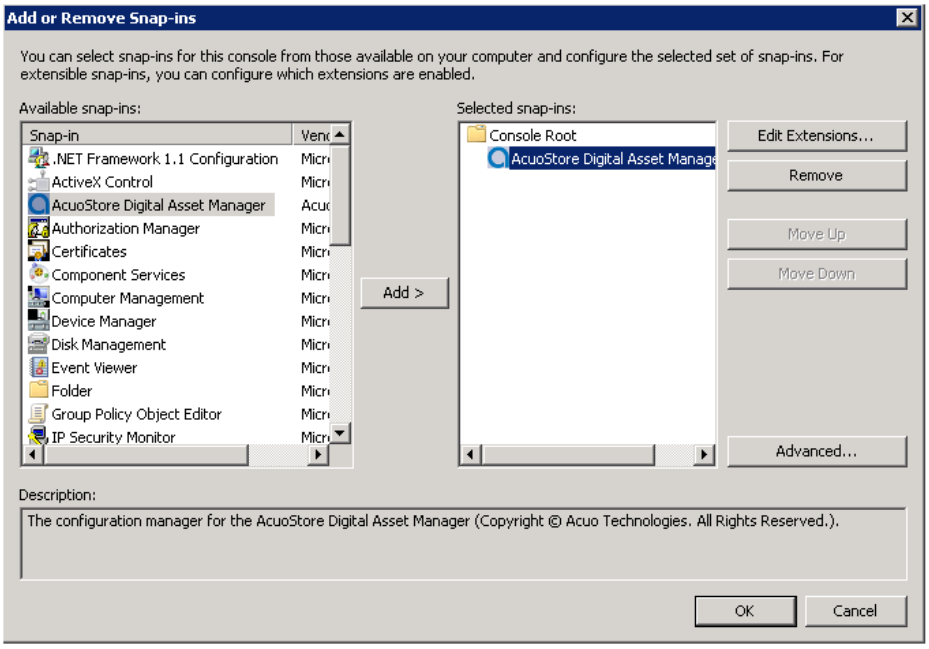
   A new blank console displays.

NOTE: If creating the MMC on a 64 Bit Operating System, in the Run dialog, type MMC -32 and click ok.



3. From the Console menu choose **Add/Remove** Snap-in.

   The Add/Remove Snap-in dialog displays.

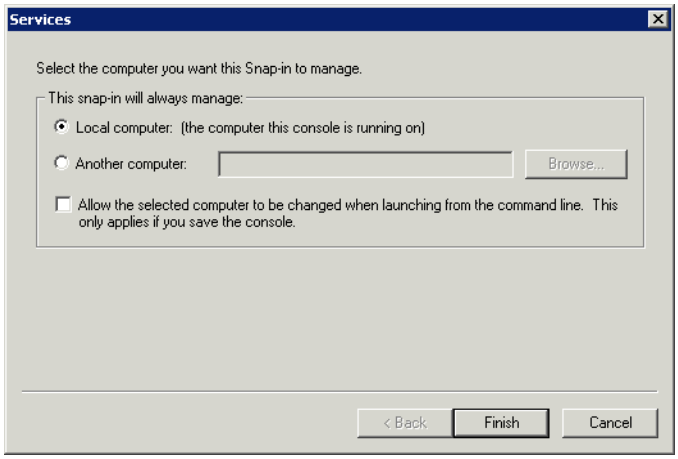


4. Locate and click the **AcuoStore Digital Asset Manager** snap-in to select it and click **Add**.

   The AcuoStore Digital Asset Manager is added to the Snap-ins list in the selected snap-ins dialog.

5. Locate and click the **Services** snap-in to select it and click **Add**.

   The Services dialog displays. The services snap-in is used to start, stop, and configure Windows services. Since AcuoStore and AcuoMed run as Windows services, you need to use the Services snap-in to manage them.



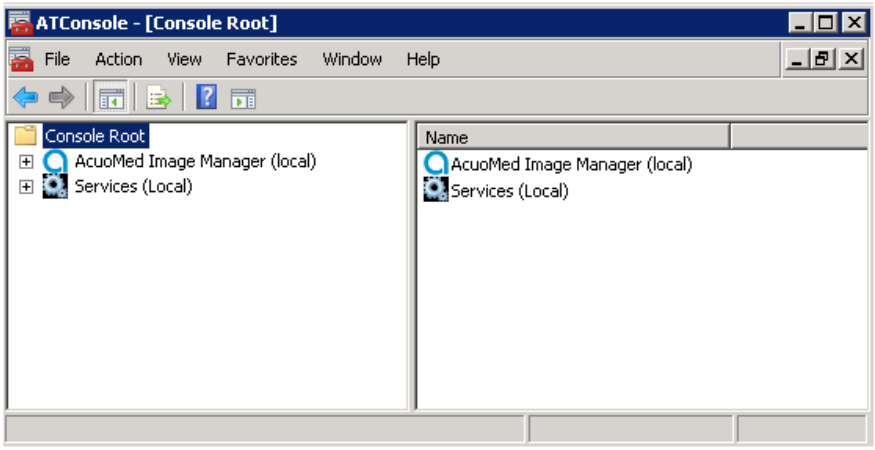
6. To have this console manage the local computer, select **Local computer** and click **Finish**.

7. (Optional) To have this console manage a remote computer, select **Another computer**, type the path (or Browse and select the path) to the remote computer, and click **Finish**.

8. (Optional) You can add any other snap-ins you may need for your application environment or for system management to the Acuo Console you are creating (for example, AcuoMed Image Manager (or other client application), Microsoft SQL Enterprise Manager or Removable Storage Management).

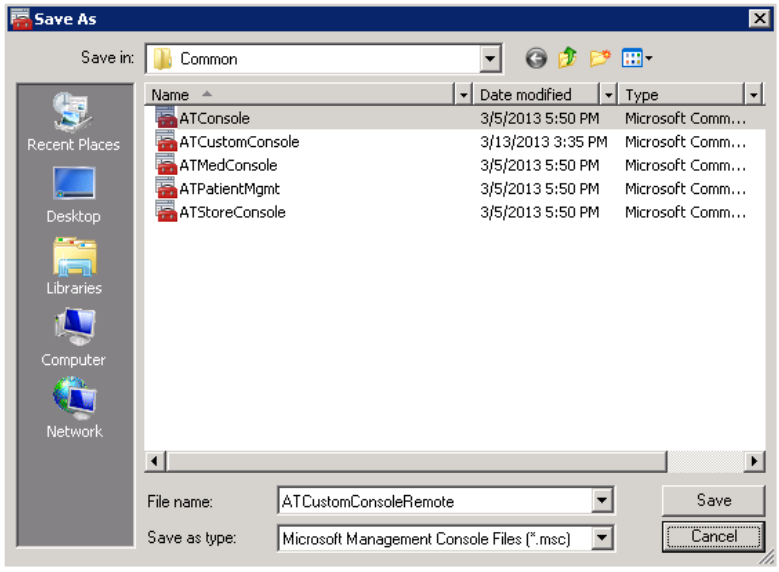
9. Click **OK** to close the Add/Remove Snap-in dialog.

   You now should see the snap-ins you added in the Console Root tree (as shown below).



10. To save your new console, click the **Console** menu and choose **Save As**.

    - The default "Save in" folder Administrative Tools is fine unless you have a reason to change it.
    - File name – a file name that is a combination of a console name and a system name is a good choice. In our example below, the existing local console "ATCustomConsole" already exists and we are adding the new console "ATCustomConsoleRemote" that will be used to manage a remote system.



11. Test to see that the newly created and saved console shows up under Start Menu→ Programs→ Administrative Tools.
12. Create a shortcut on your desktop to the new console by right-clicking it in the Start Menu and clicking Create Shortcut in the pop-up menu.

    A shortcut icon is placed on your desktop.
13. (Optional) Rename the desktop shortcut as desired.

Restarting the AcuoStore Services after Configuration

After you make changes to the AcuoStore configuration, you must restart the AcuoStore Service in order for the changes to take effect.

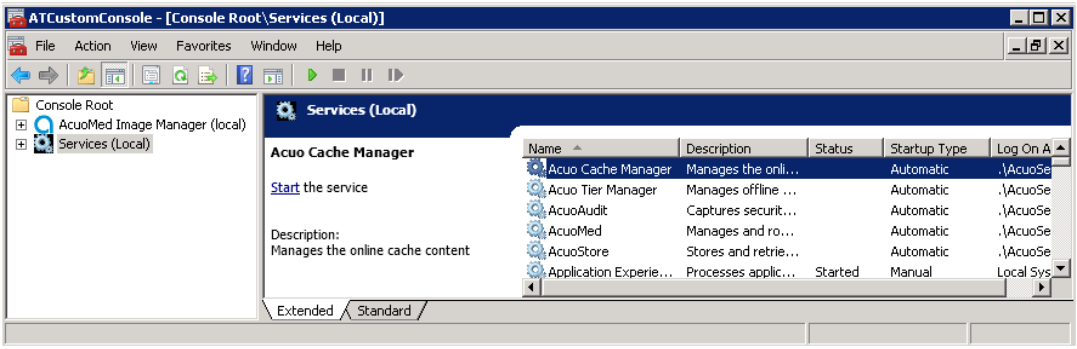
Caution

The client application (in our example AcuoMed) must be stopped prior to restarting the AcuoStore Service.

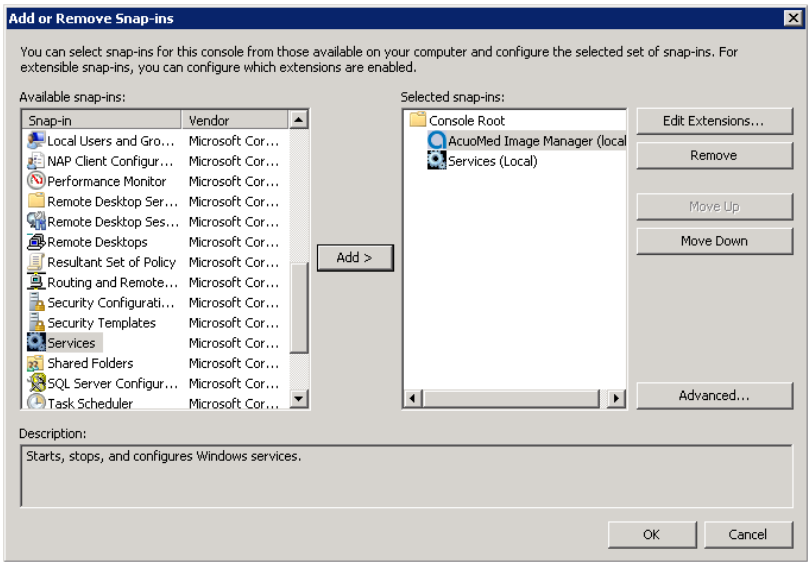
To restart the AcuoStore Service, follow these steps:

1. Verify if the Services snap-in is already added to the AcuoConsole.

   If it is already added, the Services snap-in appears in the Acuo MMC console tree as shown below (continue at Step 3). If the Services snap-in does not appear in the console tree, continue with Step 2.



2. Add the Services snap-in if not already in the console tree.
   1. From the Console menu, select **Add/Remove Snap-in**.
   2. In the Add/Remove Snap-in dialog, click **Add**.
   3. In the Add Standalone Snap-in dialog, click the **Services** snap-in in the Available Standalone Snap-ins list and click **Add**.



3. Select whether the snap-in will manage the Local computer or Another computer and click **Finish** to add the Services snap-in to the AcuoConsole.

4. In the console tree, click the **Services** snap-in to display the list of services in the right pane.

   Refer to the screen sample in Step 1.

5. In the right pane, locate and right-click the **AcuoStore and/or Acuo Tier Manager Service**.

   CAUTION: Before doing the next step, be sure that the client application has been stopped.

6. From the pop-up menu, select **Restart**.

   Windows reports progress as it Stops and then Starts the service.

   Note: You could also perform separate Stop and Start operations by selecting these options from the pop-up menu. But the Restart option performs Stop and Start in a single step.

Database Installation

Database installation includes both creating a database and connecting to the newly created database. For SQL databases, connection happens automatically as part of the installation process.

Allow plenty of disk space when installing your databases. It is recommended that you install your database on a RAID1+0 that has at least 50 gigabytes of available space. This RAID should be separate from the RAID that serves as the system drive, and from the RAID that is used to store images. For SQL, Acuo databases are set up by default to grow automatically in 1 megabyte increments. This allows the databases to start small and then grow as needed. For a more accurate configuration, please use the Acuo Volume Analysis found on www.acuotech.com.

NOTE: When upgrading your current installation of AcuoStore, it is necessary to uninstall the current product version (via Windows Add/Remove Programs) before installing the new product version. The uninstall operation does not remove any currently installed databases that AcuoStore is using. However, it will be necessary to reconnect to these databases after you have installed the new version of the AcuoStore product. Refer to the topic *Changing a Database Connection* on page 41 for instructions on how to do this.

SQL Database Installation

For Microsoft SQL, you create a new database through an MMC console. You cannot install the initial database for an MMC application remotely. That is, you must install the AcuoStore database on a machine that you are actually logged onto. However, you can use Terminal Services Client to install as if you are local (logged onto) that machine. Refer to *Chapter 5 – Remote Management* on page 57 for more information.

There is one database installation required to use AcuoStore:

- AcuoStore Database – procedure given below

It is only possible to install one AcuoStore Database for an AcuoStore Digital Asset Manager.

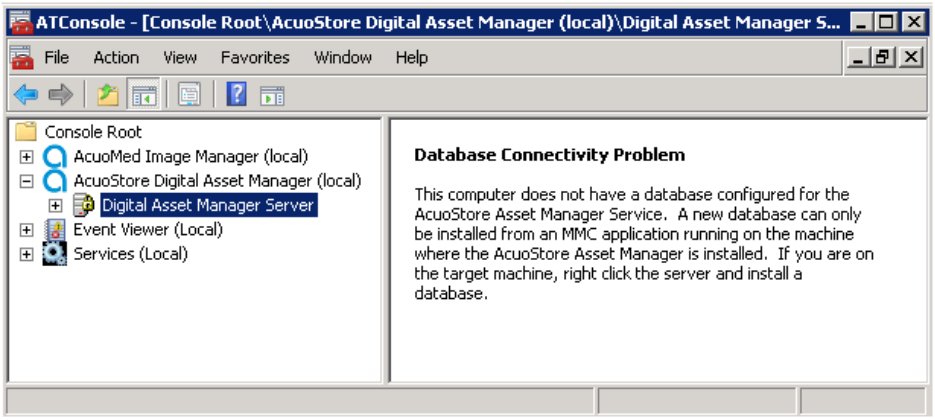
AcuoStore Database Installation

The initial installation of the AcuoStore database creates an empty database to be used by the AcuoStore Digital Asset Manager. This new database contains blank tables for Managed Shares and for Applications.

NOTE: When a new version of AcuoStore is installed, the existing AcuoStore database remains on the system. You use the "Change Database Connection" process to reconnect the existing database to the new installation of AcuoStore. Refer to the topic *Changing a Database Connection* on page 41.

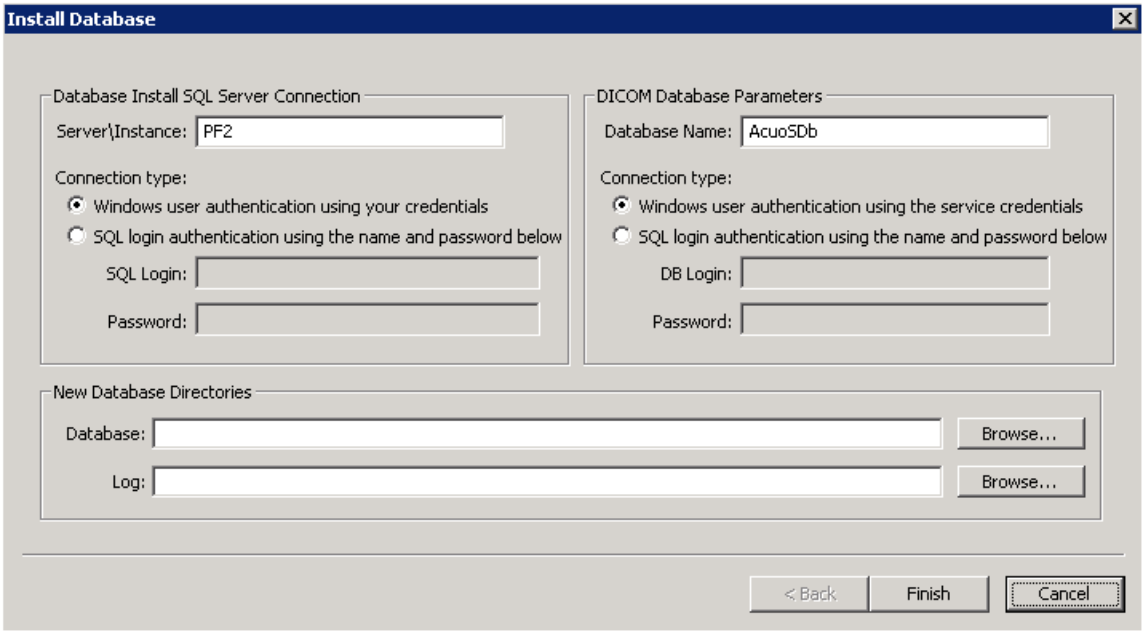
Follow these steps to perform the initial installation of an AcuoStore database.

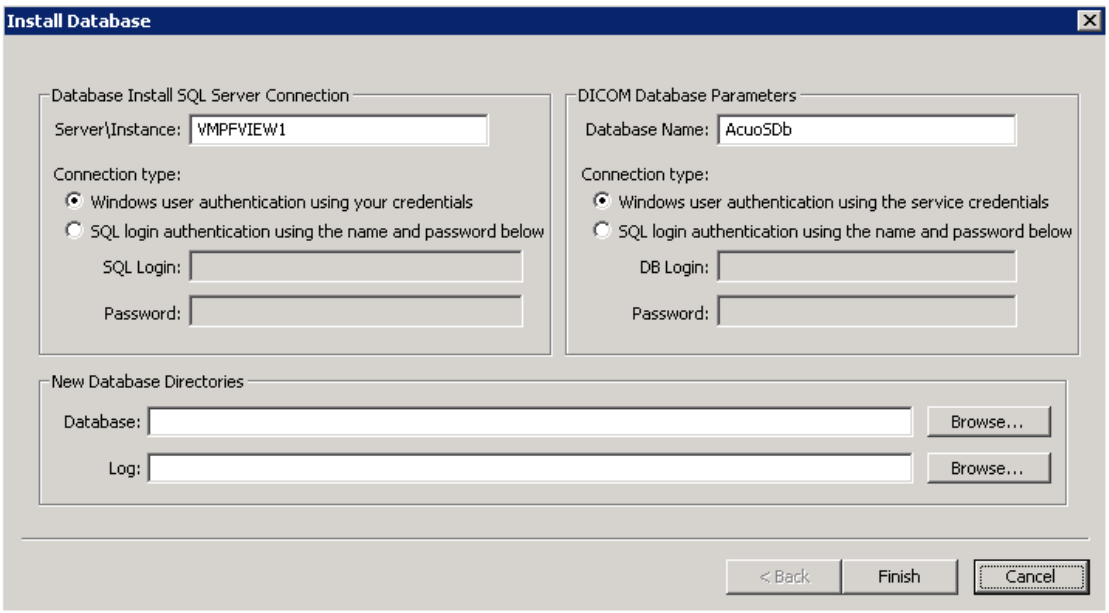
1. Start the Acuo MMC console, if it is not already running.
   - Click the shortcut on the desktop located in the Acuo Technologies Folder.
   - From the Windows Start menu, select Programs→Administrative Tools→ the Acuo MMC console.



2. Right-click **Digital Asset Manager Server** under the AcuoStore Digital Asset Manager in the console and select **Install Database**.

   The Install Database dialog displays.





3. For the Database Install SQL Server Connection section, do the following:
   - The server/instance is automatically shown as the default SQL Server Instance.
   - Select a connection type:
     - Windows User Authentication – use the current user's Windows credentials.
     - SQL Authentication - enter your unique SQL Server administrative login and password. (This is the administrative authentication that allows you to install a new database in the Database Server.)
4. For the DICOM Database Parameters section, do the following:
   - Database name: enter a name for the new database. You can use AcuoSDb or some other name that you prefer for your installation.
   - Select a connection type:
     - Windows User Authentication – database will be created using the current user's Windows credentials.
     - SQL Authentication - enter the desired SQL database login to be created with the Database.
5. Set the New Database Directories to determine where the database files will be installed.
   - Database: you can either type in a location or click **Browse** and select an existing location. Do not install database files to your system drive (where your Windows installation is located), because it is not possible to span volumes to expand the system drive as your database grows. Instead, install the database on a separate partition or different physical drive.
   - Log: Microsoft recommends that you save log files on a different drive than where the database files are saved (but this is not a strong recommendation); so, you can save them in the same directory as the database files if you prefer.
6. Click **Finish** to complete the installation.

   You can verify that the database is installed and connected. In the MMC console tree, click **AcuoStore Digital Asset Manager** to select it. In the right pane for the AcuoStore Server/Database Server, you should see a Configuration Database Status of **Connected**.

Changing a Database Connection

Changing a database connection allows you to connect to an AcuoStore database that has already been installed on the system.

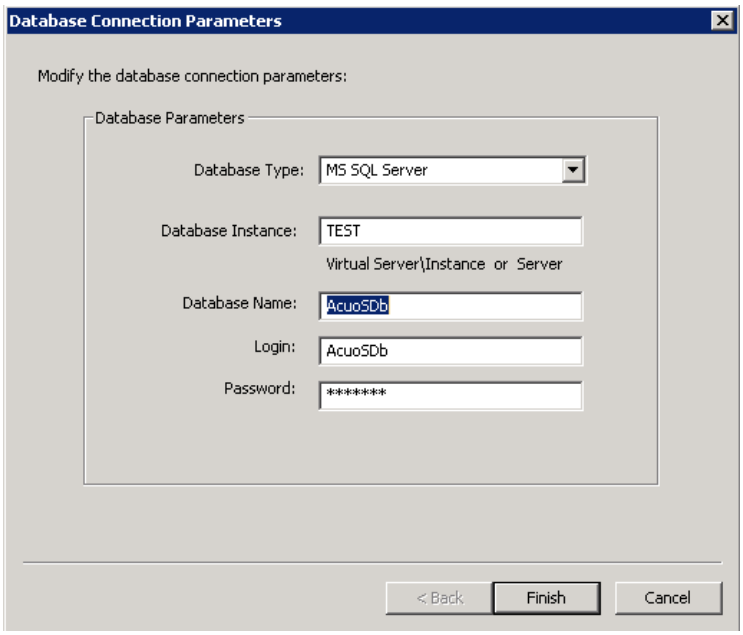
- **SQL databases** – database connection is done automatically as part of SQL database installation. So the Changing a Database Connection procedure is not needed following installation of a **new** SQL database. However, when an AcuoStore application **upgrade** is installed, it is necessary to reconnect to existing SQL databases by means of the Changing a Database Connection procedure, unless upon uninstalling the old version of AcuoStore, you answered "yes" to the following question, "Do you wish to save the current AcuoStore Digital Asset Manager settings for reinstallation?"

Follow these steps to change a database connection (connect/reconnect) to an AcuoStore database:

For AcuoStore, it is only possible to have one AcuoStore database per AcuoStore application per server.

1. In the MMC console tree, right-click **Digital Asset Manager Server**.
2. From the pop-up menu select **Change Database Connection**.

   The Database Connection Parameters dialog displays.



3. Select the Database Type from the list: **MS SQL Server**.
4. Type the Server name where the database is installed.
5. Type the Database name. This is the Database Name parameter that was specified at database installation.

6. Type the database Login. This is the Login parameter that was specified at database installation. If using Windows Authentication, leave this field blank.

7. Type the database Password. This is the Password parameter that was specified at database installation. If using Windows Authentication, leave this field blank.

8. Click **Finish** to change the database connection.

Chapter 4 – AcuoStore Configuration Example

In this chapter:

Configuration Example Overview

The example configuration in this chapter demonstrates how to set up AcuoStore to fulfill the basic needs of a typical implementation. AcuoStore has just two primary components that need to be configured — Managed Shares and Applications. Once you have configured these, AcuoStore allows you to check digital assets into and out of the storage archives that you selected in your configuration.

Before configuring AcuoStore, you must have completed the following tasks:

- Installed AcuoStore and an AcuoStore database and created an MMC console according to the corresponding procedures found in *Chapter 3 – Getting Started* beginning on page 24.
- Analyzed the storage needs of your client application, for example AcuoMed, and obtained and placed online the storage devices necessary to support those needs. (In the AcuoStore configuration procedure that follows there is a step that allows you to specify how much space to use on a given storage device. It follows naturally then, that you should have already assessed how much space you need and obtained devices sized to meet those needs.)
- IMPORTANT: Using standard Windows techniques, set up a share to the storage device on which you intend to store digital images.

NOTE: In Windows, administrators must manually set the permission and security on each folder shared. Right-click on the folder to share → select properties → click on tab for sharing → click on box for permissions and give full control to the users Acuo Administrators and Acuo Power Users. Give read-only access to Acuo Users. These groups are installed upon installation of the service.

As is shown in Figure 7, AcuoStore and the client application (for example AcuoMed) are installed on the same server, and AcuoStore is mapped to the local image cache on a one-to-one basis. Note that if for some reason you have more than one local image cache on your server, you must map all local image caches to the same AcuoStore. Also, depending upon the needs of your implementation, AcuoStore and the client application can be installed on different servers.

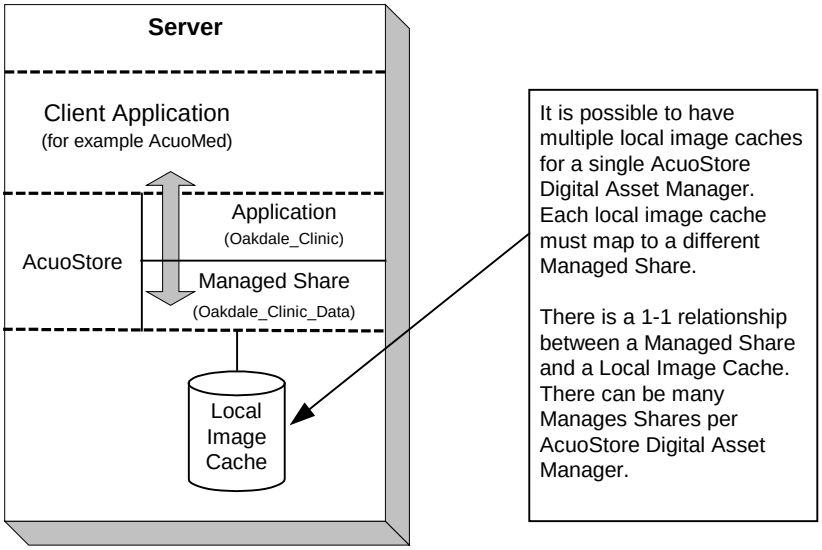


Figure 7: Detailed view of the configuration example

Also shown in Figure 7, is that one managed share and one application are set up to create a linkage to the storage area on the local image cache. The one managed share, named Oakdale_Clinc_Data, is associated with the one application named Oakdale Clinic. This application will be limited to using 10 gigabytes of physical disk space. The following procedures demonstrate how to set up the example configuration described above.

Configure Archive Device

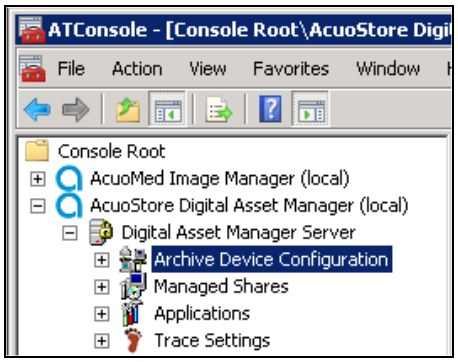
AcuoStore currently supports several Archive Devices. The types of Archive Devices supported in this release are as follows:

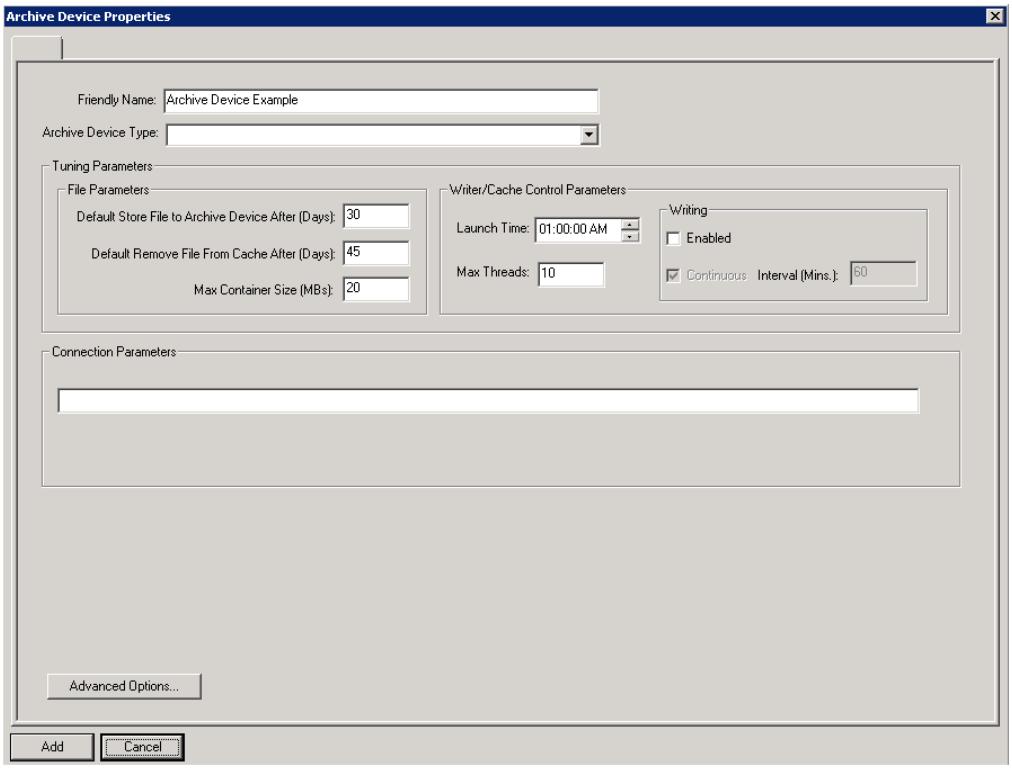
- EMC Centera
- EMC Atmos
- NetApp/Bycast
- Dell – DX
- Dell Cloud
- Hitachi
- Nirvanix
- Scality
- FileStore

The Steps below outline the process for configuring the supported devices.

Configure an Archive Device

To connect a server to an archive device, from the Acuo MMC console main dialog, right-click **Archive Device Configuration** and select **New→ New Archive Device Configuration.**





1. In the Friendly Name field, type a name (no longer than 64 characters) for the device.
2. Select the device from the Archive Device Type dropdown menu.

   The options in 6.0 are listed below:

   - EMC Centera
   - EMC Atmos
   - NetApp/Bycast
   - Dell – DX
   - Dell Cloud
   - Hitachi
   - Nirvanix
   - Scality
   - FileStore

3. Configure the Archive Device Tuning Parameters.

   File Parameters are global default values. These values are inherited when a new Application is created. (they can be modified when the Application is created or at a later time.)

   - Default Store File to Archive Device After (Days): (Default is 0) → File is considered Nearline. NOTE: Recommend changing this setting to 1.
   - Default Remove File From Cache After (Days): (Default is 7) → This number must be greater than the Store File to Archive Device number. File is considered Offline.
   - Max Container Size (MBs): (Default is 20) → Parameters are 5 - 100 (MBs).

   Writer/Cache Control Parameters indicate the time each day a list of files (within the max container size) will be written to the archive device. After successful write to the Atmos device, a CLIP ID will be entered into the archive location column of each file in the list.

   - Launch Time (Default is 1:00:00 AM) → The daily time that data will begin to store to the archive device. Correlate this time with your SQL maintenance job schedule so that both are not running at the same time.
   - Max Threads (Default is 10) → Indicates the total number of threads that can be open to the archive device at any given time. Please contact Acuo Technologies for assistance with this advanced parameter.
   - To indicate a time interval in which to continuously write files to the archive device, select Enabled under **Continuous Writing** and specify the time (in minutes) to use as the interval.

Connection Parameters

The Connection String is the list of IP addresses and Port of the archive device. The connection string is obtainable from the Field Service personnel.

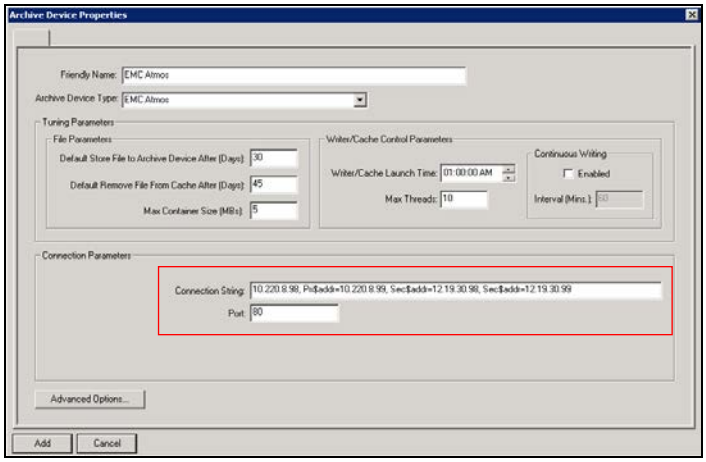
Primary/Secondary IPs

AcuoStore has the ability to distribute load evenly to multiple nodes, and reference a set of secondary nodes (or IPs) if primary nodes are unavailable.

The primary means of communication to an archive device's storage grid is through a Communication Load Balancer (CLB). This node is aware of the state of all storage nodes in the grid and directs traffic to an appropriate storage node for service. If a particular storage node is momentarily overloaded or offline, the CLB will direct traffic to an alternative storage node. This frees AcuoStore from having to query the grid to find appropriate endpoints to communicate with.

The "URL" or "Conntection String" field contains the primary and secondary nodes. Primary nodes are specified by '**Pri$addr**' and secondary nodes as '**Sec$addr**'. An IP address with no designation will be a primary address by default (making it possible to run on an existing system with new software without reconfiguring). The connected Archive Device must support multiple IP addresses. Please reference the screenshot below.

In the example below, 10.220.8.98 and 10.220.8.99 are the primary nodes. 12.18.16.98 and 12.18.16.99 are the secondary nodes.

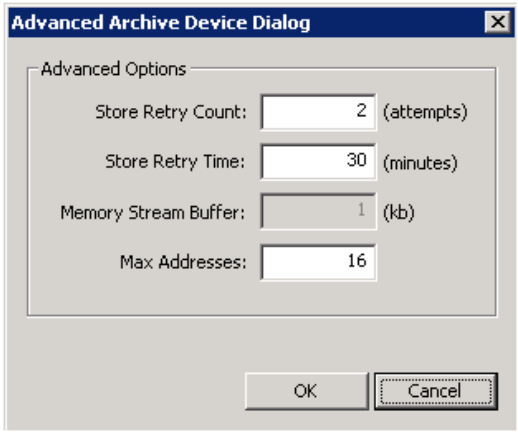


Default Security Parameters

The Default Security Parameters contain credentials necessary for access to the certain Archive Devices. Values entered in the Archive Device configuration are defaults and will auto-populate when creating new AcuoStore Applications. These parameters include:

- SubtenantID/UID – (i.e., Atmos, Hitachi, Nirvanix, Scality)
- Shared Secret – (i.e., Atmos, Hitachi, Nirvanix, Scality)
- Application Key – (Niranix)
- Application ID – (Nirvanix)
- Bucket Name – (Scality)

4. (Optional) Advanced Archive Device Options gives additional configuration options for AcuoStore as follows:



- Store Retry Count (default 2 attempts) - The number of times AcuoStore will attempt to write data.
- Store Retry Time (default 30 minutes) - The interval in time between the Store Retry Count when AcuoStore will attempt to write data.
- Memory Stream Buffer (default 16 kb) - This shows how big each piece of data is that is being sent. (This is grayed out at all times.)
- Max Addresses (default 16) - This sets the maximum number of addresses allowed.

AcuoStore Services Grid

The Acuo Tier Manger and Acuo Cache Manager services are created at the time of install/upgrade and are disabled by default. The Tier Manager Service is responsible for orchestrating the writing of assets to offline storage devices. The Acuo Cache Manager is responsible for removing assets from the local cache once they have been successfully written offline. The segregation from the AcuoStore service will allow for improved efficiency, flexibility and compatibility with an increasing number of Archive Devices. Please view the grid below for detailed information regarding the installed services and their responsibilities based on the type of CAS Device being used.

This table below illustrates the recommended state of Acuo Services depending on the configuration implemented.

Configuration/Archive Device	**Service State**			
	AcuoStore	**AcuoMed**	**AcuoAudit**	**Acuo Tier Manager**
No Archive Device	Enabled	Enabled	Enabled	Disabled
Acuo with Archive Device				
EMC Centera	Enabled	Enabled	Enabled	Disabled
Any Other Non-Centera Device	Enabled	Enabled	Enabled	Enabled
Dedicated Writers				
EMC Centera [1]	Enabled	Disabled	Disabled	Disabled
Any other Non-Centera Device	Disabled	Disabled	Disabled	Enabled

[1] When writing to EMC Centera devices, If there are multiple AcuoStore systems using the same AcuoStore Database, only 1 should be configured. In this setup only 1 system should have the registry setting "CASWriter" set to a value of 1.

The table below illustrates the Acuo Service Responsibilities when using an archive device.

Archive Device	**Service Responsibilities**		
	File Writer	**Acuo Cache Manager**	**Orphan Sweeper**
EMC Centera	AcuoStore	Acuo Cache Manager	AcuoStore
Any other Non-Centera Device	Acuo Tier Manager	Acuo Cache Manager	AcuoStore

Please note that a restart of both the AcuoStore and Acuo Tier Manager Service is required in order to accommodate any modifications made to either configuration. This is important to remember especially in implementations where the writer is hosted separately.

Configuring Managed Shares

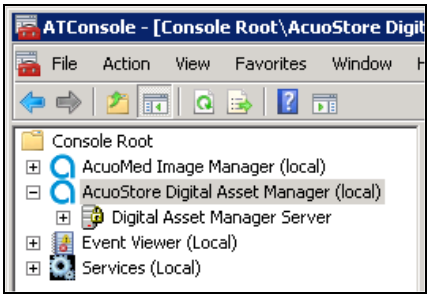
To set up AcuoStore, configure managed shares before configuring applications. As described in Chapter 2, managed shares are logical mappings to physical storage space that function like conduits through which digital assets flow to and from specific storage devices.

NOTE: To complete this procedure, ensure that you have completed the bulleted tasks noted in the previous topic, *Configuration Example Overview*. For more information, refer to the topic *Managed Shares* on page 16.

Follow these steps to configure a managed share.

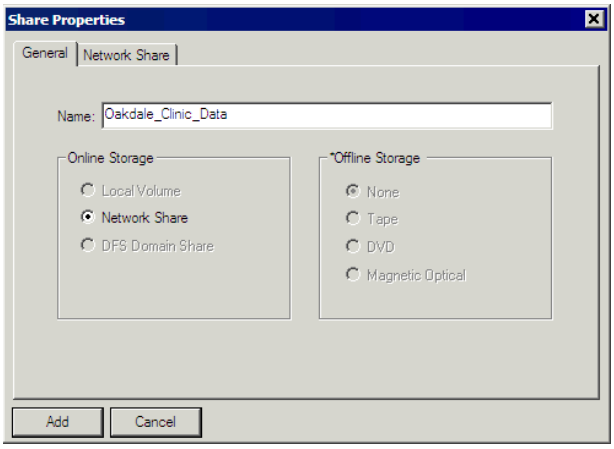
1. Start the Acuo MMC console, if it is not already running.
   - Click the shortcut on the desktop, if there is one, or
   - From the Windows Start menu, select Programs→Administrative Tools→ AcuoStore Digital Asset Manager.

   The Acuo MMC console displays.

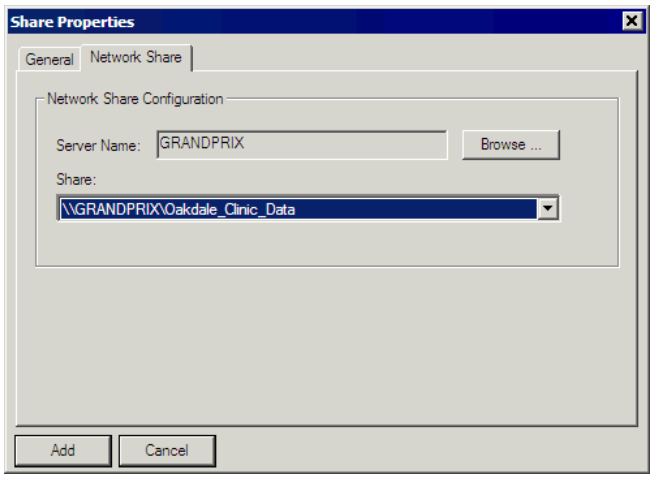


2. Expand the console tree as follows: AcuoStore Digital Asset Manager→Digital Asset Manager Server.
3. From the Acuo MMC console tree, right-click **Managed Shares** and select **New→ New Share**.

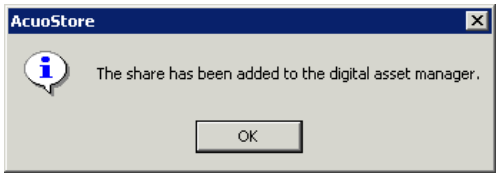
   The Share Properties dialog displays with the General tab selected.



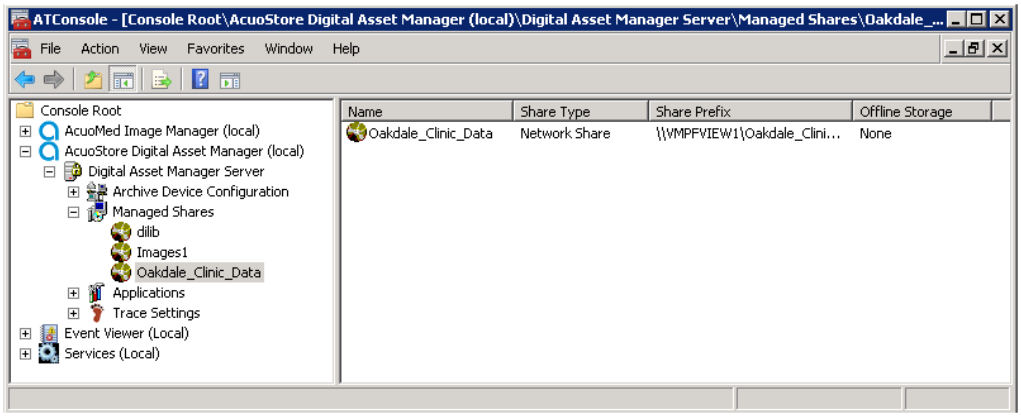
4. Using the General tab, set up the following parameters:
   - In the Name field, type the name of the new share (Oakdale_Clinic_Data in our example).
   - For Online Storage type, click the applicable radio button.
   - Select an offline storage type if applicable
5. Click the **Network Share** tab to continue.



6. The default Server Name is your local machine by default. If your physical NTFS shares reside on a different server, browse your network for that server.
7. From the drop-down list, select the storage device on which you set up a share.
8. Click **Add** to configure the managed share and add it to the archive.



This completes the procedure to configure a managed share. The new managed share (Oakdale_Clinic_Data) now appears in the console tree as shown below.



Repeat this procedure to create additional managed shares, or continue with the next procedure to configure applications.

Configuring Applications

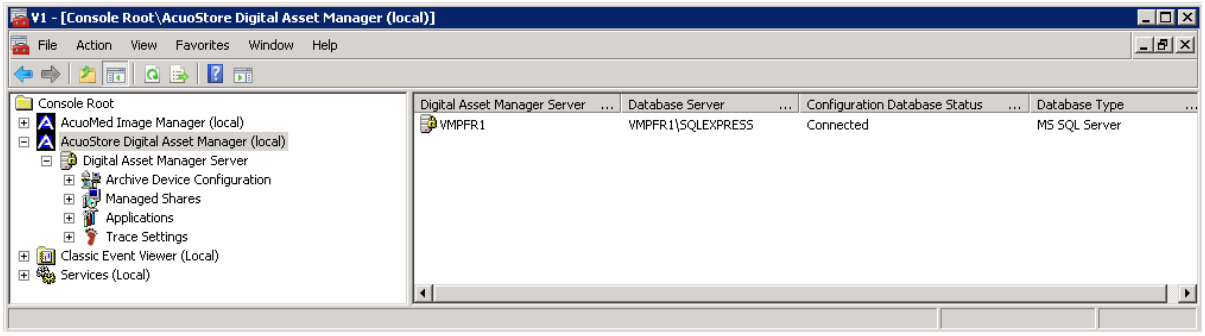
Once you have configured at least one managed share, you can configure applications. As described in Chapter 2, applications let you control which subscribers have access to a managed share and how much space each subscriber can use on the share.

NOTE: To complete this procedure, ensure that you have completed the bulleted tasks list in the topic, *Configuration Example Overview* on page 43. For more information, refer to the topic Applications on page 20.

Follow these steps to configure an application.

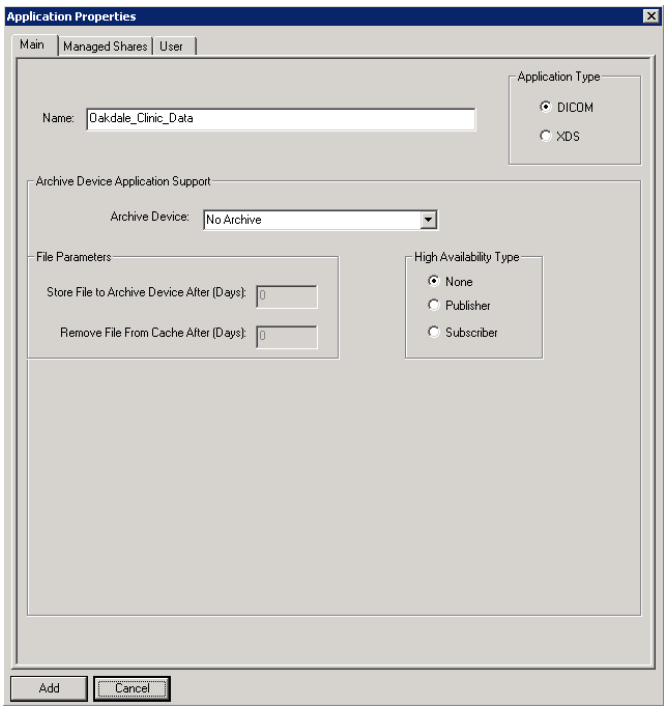
1. Start the Acuo MMC console, if it is not already running.
   - Click the shortcut on the desktop, if there is one, or
   - From the Windows Start menu, select Programs→Administrative Tools→ AcuoStore Digital Asset Manager.

   The Acuo MMC console displays.



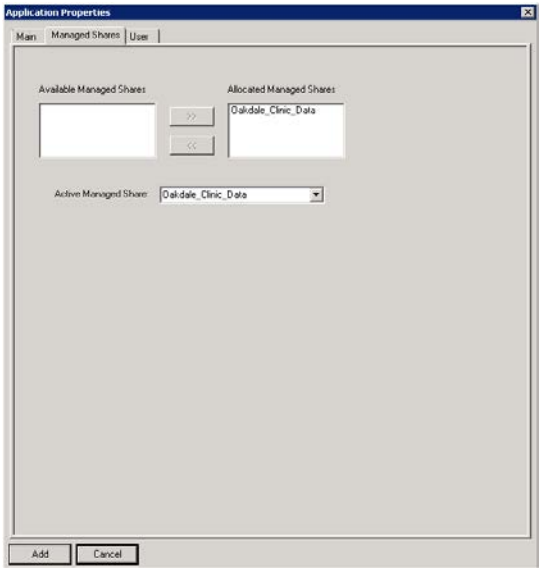
2. Expand the console tree as follows: AcuoStore Digital Asset Manager→AcuoStore Server.
3. From the Acuo MMC console main dialog, right-click **Applications** and select **New→ New Application**.

   The Application Properties dialog displays with the Main tab selected.



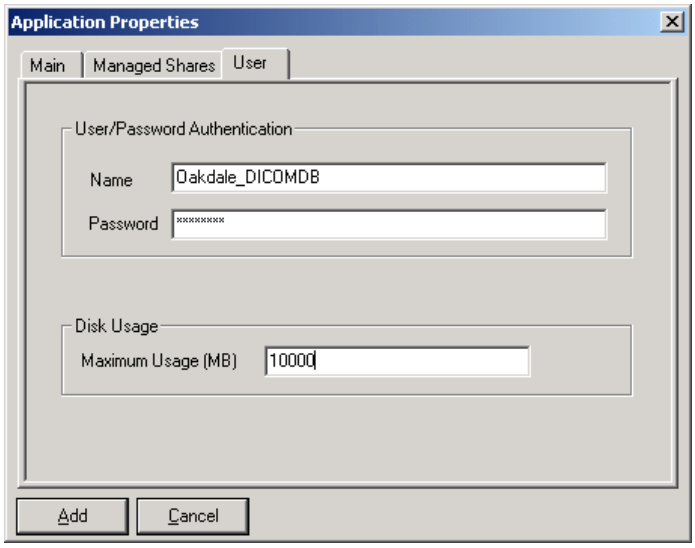
4. Using the Main tab, set up the following parameters:
   - In the Name field, type the name of the new application (Oakdale_Clinic in our example).
   - Select the Application Type: (DICOM or XDS)
   - If there is a connected archive device, check **Use Archive Device** and change the default File Parameters. If connected to an archive device that requires login credentials, enter before continuing. (See screenshot above). For more information on configuring an Archive Device, see the Configuring Archive Device section.

5. Click the **Managed Shares** tab and set up the allocated shares.



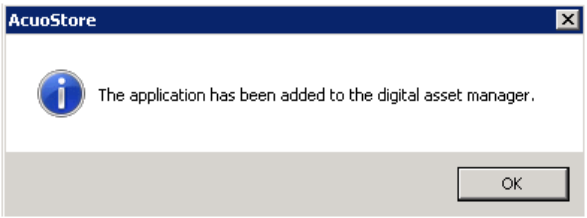
   - Move the share(s) that you want to allocate from the Available Managed Shares list to the Allocated Managed Shares list. Data will write to the **Active Managed Share**.

6. Click the **User** tab to set up the application user.

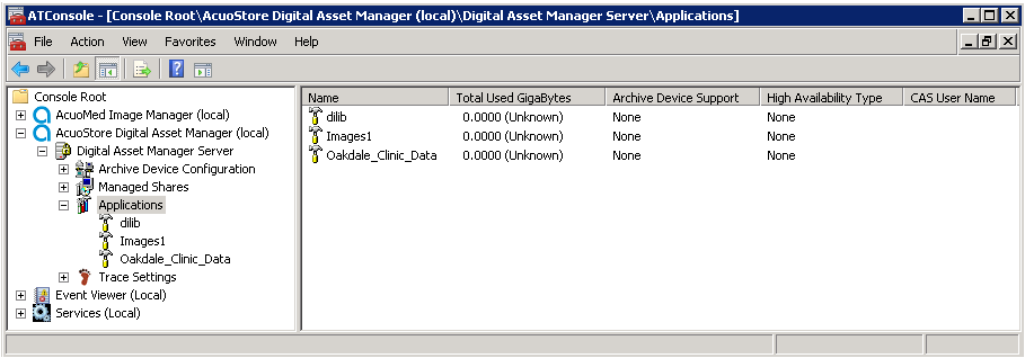


- Type the user authentication Name (Oakdale_DICOMDB in our example) and Password.
- For Disk Usage, type the maximum disk space that will be allowed for this application (10000 MB, which is 10 gigabytes, in our example). Entering 0 in the Maximum Usage field allows for unlimited disk space.

7. Click **Add** to configure the application and add it to the archive.



This completes the procedure to configure an application. The new application now appears in the console tree as shown below.



Repeat this procedure to create additional applications, or continue with procedures to configure your client application. Refer to the *AcuoMed Installation and Operations Guide*, Chapter 4 for the AcuoMed configuration example.

Configuration Example Conclusion

The example configuration detailed in the previous topics is simple and only one out of many possible configurations. However, even if a number of options were changed, the example configuration shown above would still clearly demonstrate how to configure AcuoStore and how simple and easy it is to use. Refer to the topics *Managed Shares* on page 16 and Applications on page 20, as well as the online Help system for detailed information about the options you can select while creating managed shares and applications.

Chapter 5 – Remote Management

In this chapter:

Overview

Remote management refers to the practice of managing a computer at a different physical (remote) location from a local computer. Practically speaking, remote management lets you manage an Acuo server at one or more remote locations (for example, at several clinics or imaging centers) from another remote location (such as a central hospital). This AcuoStore discussion of remote management is done in the context of the AcuoMed client application, but the same concepts would apply for a client application other than AcuoMed.

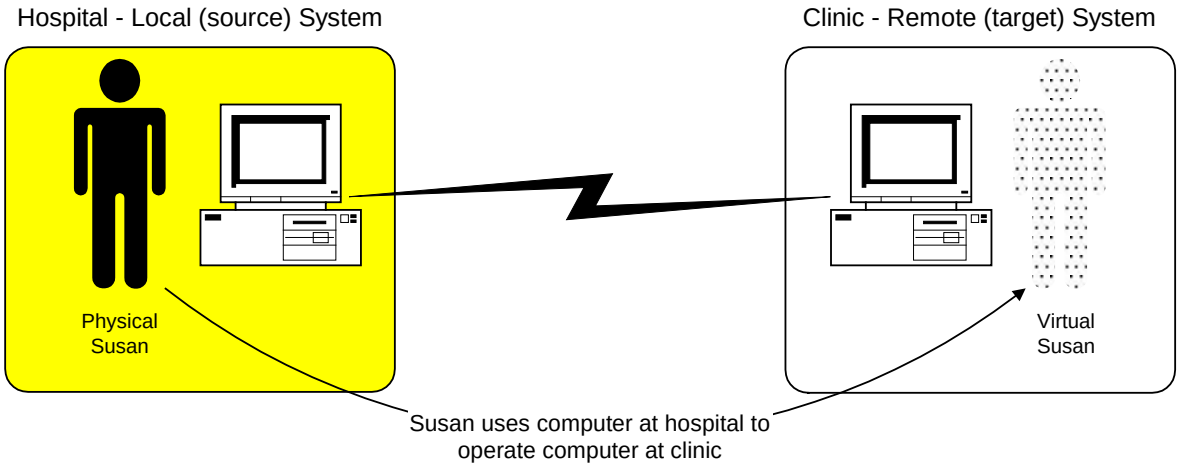


Figure 8: The remote management concept

NOTE: In the topics that follow, the term *source system* refers to the local system being used to manage a remote system. The remote system being managed is referred to as the *target system*.

There are two methods of administering remote management that essentially perform the same functions. However, each method has certain characteristics that make it distinct from the other. These methods, and their differences, are described under the following two topics:

- Management via MMC Console
- Management via Terminal Services Client (Terminal Server)

Management via MMC Console

Setting up an MMC console on a local server to manage a remote server eliminates the need to physically be where the remote server is located in order to perform certain tasks on it. Instead, you can manage other MMC console services and perform certain tasks through those services on remote servers from virtually any local server. Typically, these tasks include:

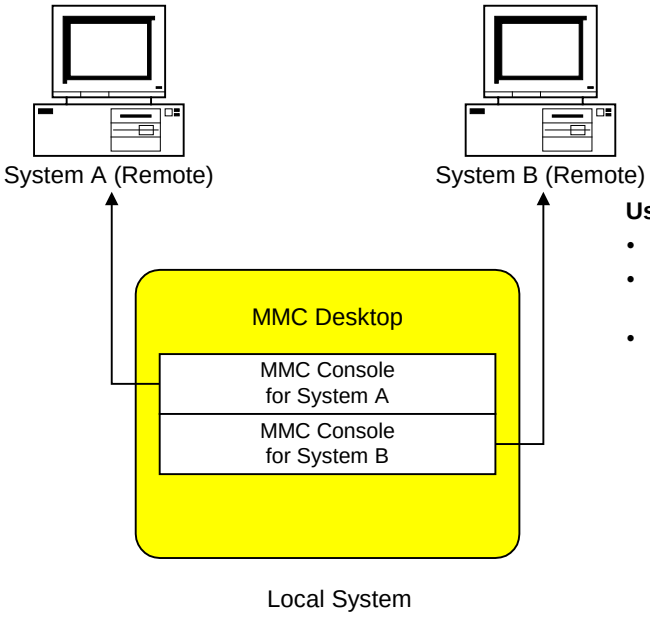
- Changing the configuration on the remote servers
- Stopping and restarting services on the remote servers
- Setting up a group of snap-ins that you want to routinely manage on the remote servers

NOTE: Management via MMC Console requires that the local server has a high-speed, highly available connection to the remote server. If this is not the case, Management Via Terminal Services Client is the better choice (refer to the discussion of this topic on page 65).

MMC Operational Considerations

The MMC console method of managing systems remotely is the preferred method if you have MMC supported Windows operating system running on both the local and remote systems, and if you can access the local system from a remote system through a secure Intranet. If you can access the Intranet via a Virtual Private Network (VPN) using the Internet, this is also acceptable. Conversely, the MMC console method is not a viable method if at least one of your systems is not running a supported Windows operating system or if you have to go through a firewall without the benefit of a VPN.

To help determine whether using MMC console is an appropriate method for you to remotely manage other systems, review Figure 9 and the explanations that accompany it.



Using MMC Console:

- Windows 2000 required
- Log into Local System using its login ID and password
- After initial login, if System A and System B are physically on the same Intranet as the Local System, log directly into them via the MMC consoles for System A or System B
  -OR-
  After initial login, if the Local System is NOT Intranet-connected to Systems A and B (they are on the Internet instead), first log into System A or B via a VPN connection and then log in via the MMC Console for System A or B

Figure 9: Remote management using MMC console

Figure 9 shows that to manage a system remotely via an MMC console you must first log into the local system with its login ID and password. Once you are logged into the local server, you can create one or more MMC consoles to manage one or more corresponding remote servers.

In addition, Figure 9 notes that there are two access scenarios for using the MMC console approach to remote management — from INSIDE and from OUTSIDE your organization's Intranet. To summarize the difference, if both the local server and remote server are on the same Intranet, you can log directly into the remote server inside the Intranet with an MMC console application created for that purpose on the local server. Or, if the remote server is on the Internet, you must first access the remote server via a VPN across the Internet; you can then log into the remote server via an MMC console application created for that purpose on the local server. For an example of this, see the instructions with Figure 9.

MMC Configuration

The following procedure describes how to set up a local server to manage Acuo services running on a remote server.

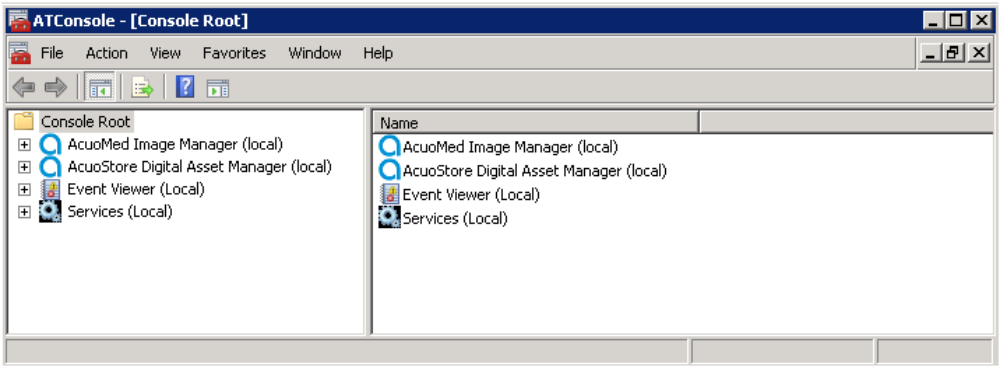
NOTE: The following procedure assumes that you have already set up an MMC console on your local server and that it is currently managing AcuoMed and AcuoStore services. If this is not the case, complete the steps in the topic *MMC Console Creation* on page 32, before starting this procedure.

IMPORTANT: This procedure also assumes that the remote server (the target server you want to manage) is either on the same Intranet as the local server or that, if you are accessing the remote server via an Internet VPN, you have already connected to the remote server via that method.

To set up a local server that will manage services on a remote server, follow these steps:

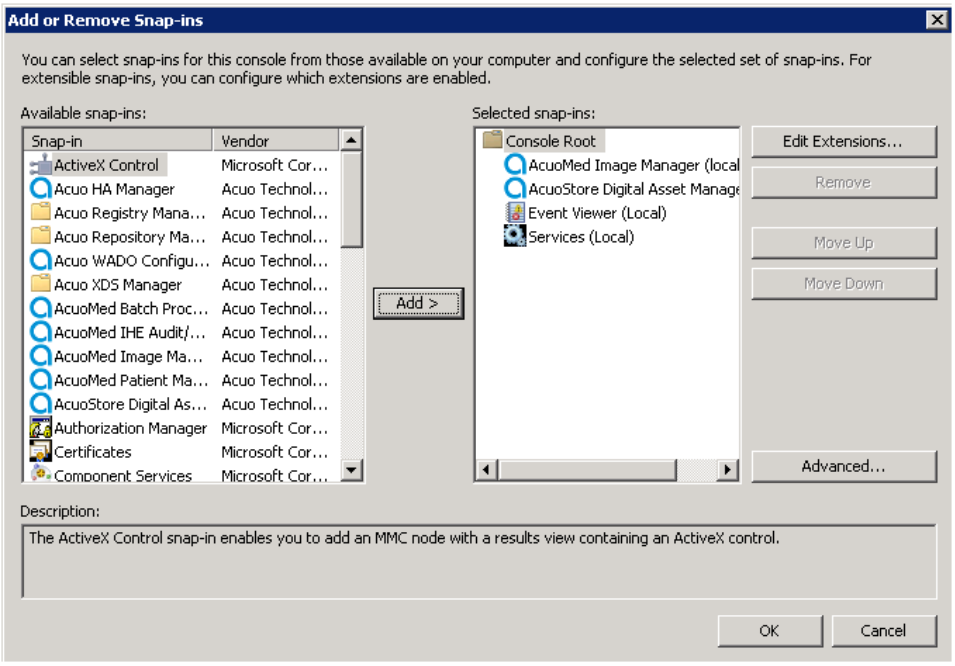
1. On the local server, open your MMC console.

   The Console Root screen displays.



2. From the Console menu, select **Add/Remove Snap-in**.

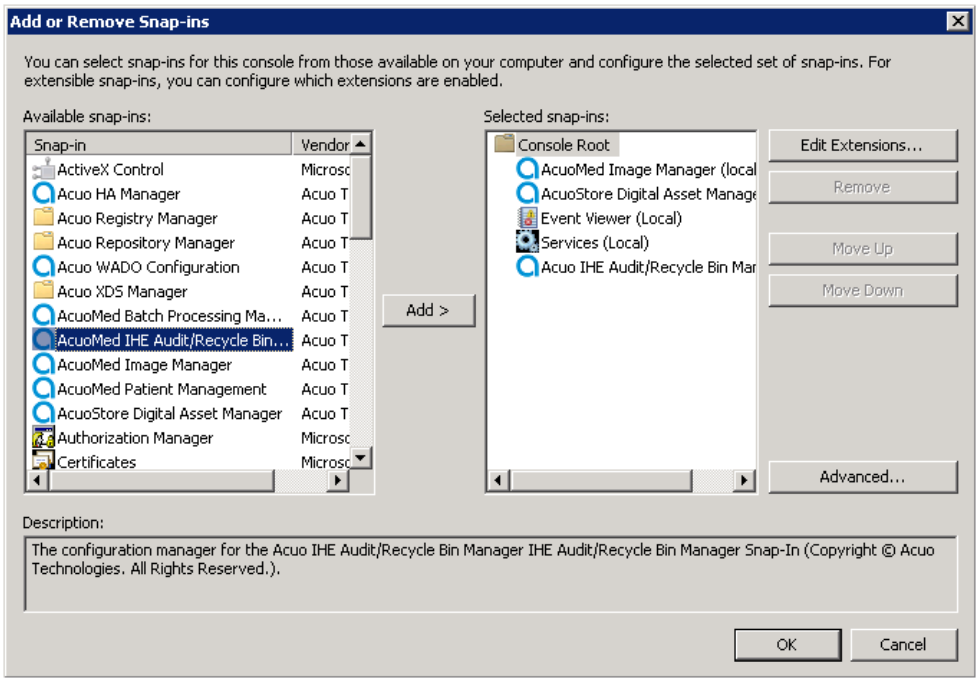
   The Add/Remove Snap-in dialog displays, which shows all the snap-ins you are running locally.



3. The Add Standalone Snap-in dialog displays.

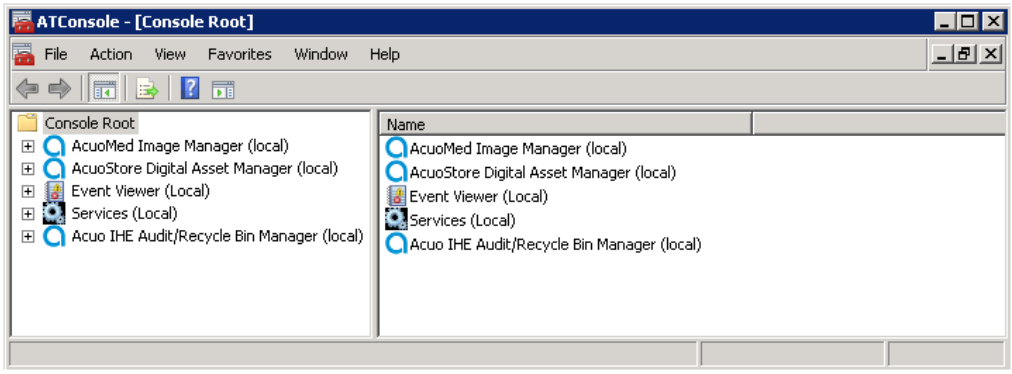
4. Using the Add Standalone Snap-in dialog, add additional AcuoStore and AcuoMed snap-ins by highlighting each snap-in and then clicking **Add**.

   When you are done adding snap-ins, the Add/Remove Snap-in dialog displays each new addition.



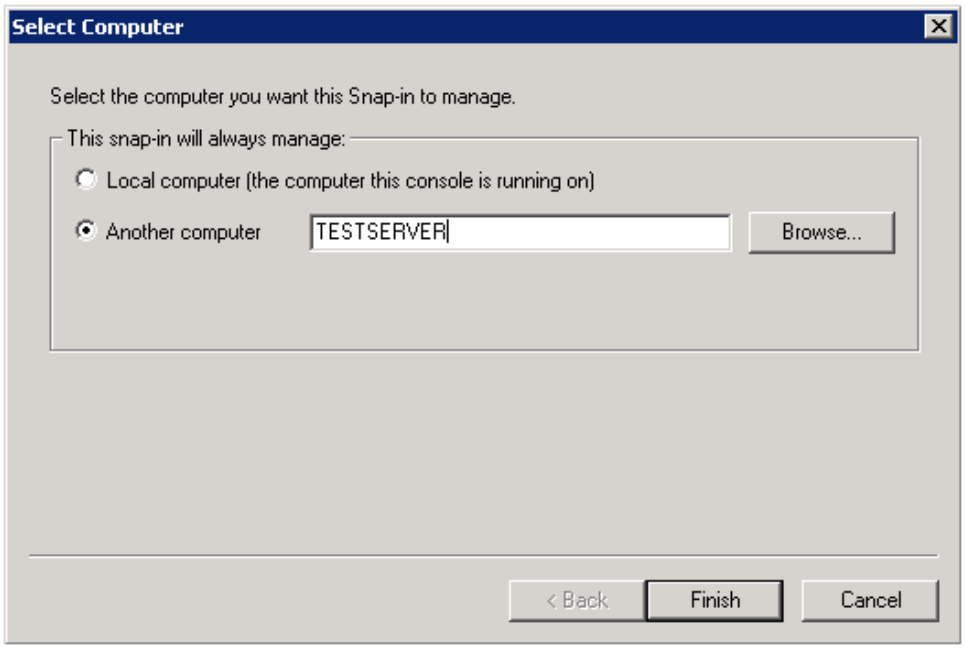
5. Click **OK** to continue.

   The Console Root screen displays, which should now show the added Snap-ins.



6. To select a different computer for a duplicated snap-in to manage, right-click the **AcuoStore Server** or the **AcuoMed Server** and select **Connect to Another Computer**.

   The Select Computer dialog displays.

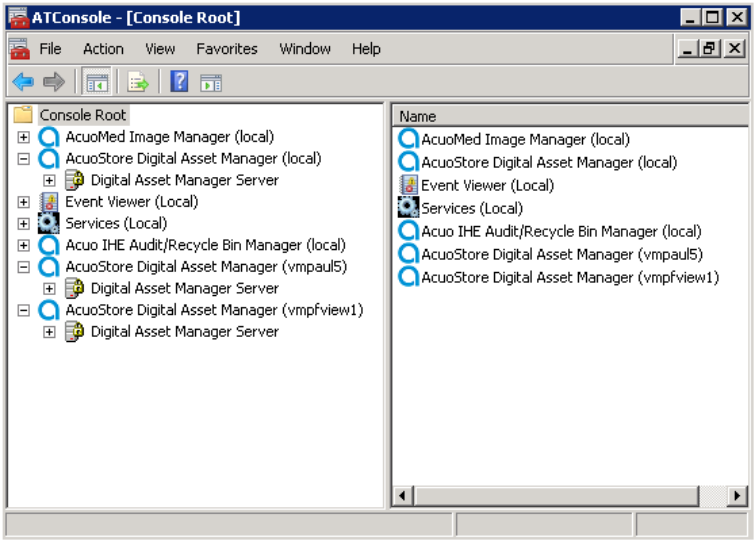


7. Click **Another Computer** to select it, click **Browse** to browse for another server, and, when you have selected the target server you want to manage, click **Finish**.

   Note: When you click **Browse**, the Browse for Computer dialog displays, which is a standard Windows browsing window that lets you attach to any server on your Intranet or VPN connection. Alternatively, if you know the name of the server that you want to connect to, type the name in the field provided, and then click **Finish**. The Console Root screen displays (see sample for Step 8).

8. Repeat Steps 6 and 7 for the second duplicated snap-in.

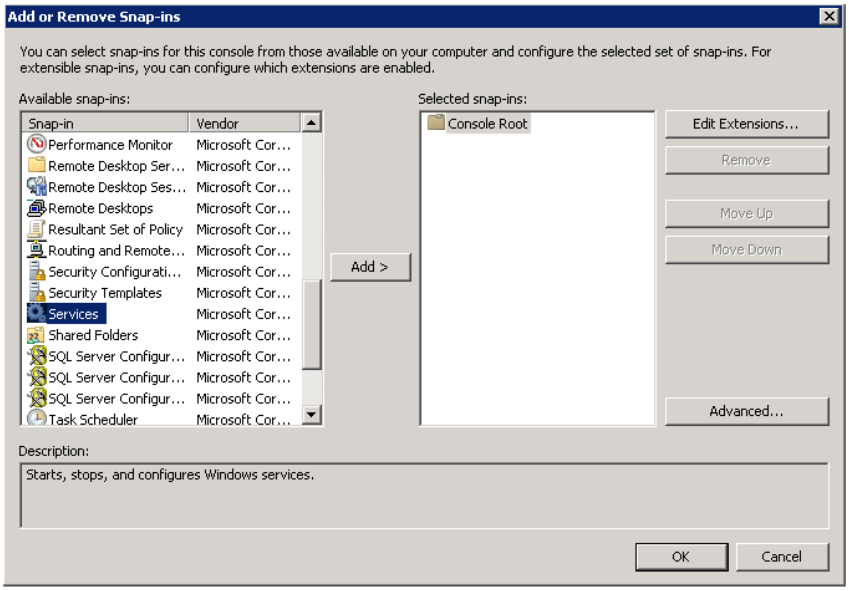
   The Console Root screen should show that the duplicate AcuoStore and AcuoMed snap-ins are now managing a different server.



9. To add an additional snap-in, for example the Services snap-in, repeat Steps 2 and 3 of this procedure and highlight the **Services** snap-in (as shown below).

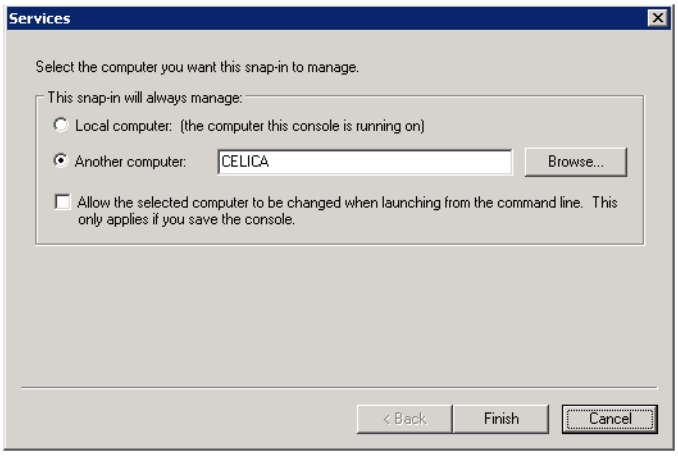
NOTE: Using the Add Standalone Snap-ins dialog, you can add the additional snap-ins that you want. Generally speaking, adding snap-ins expands functionality, which means in this context that you can increase the number of tasks you can complete on a remote (target) server. Note that all snap-ins are not added in the same manner and that a description for how to add each of them is not included in this manual. However, a description for how to add the Services snap-in is included below since it is recommended that you add this snap-in for most remote management implementations.

The Add Standalone Snap-in dialog displays.



10. Click **Add** to continue.

The Services dialog displays.

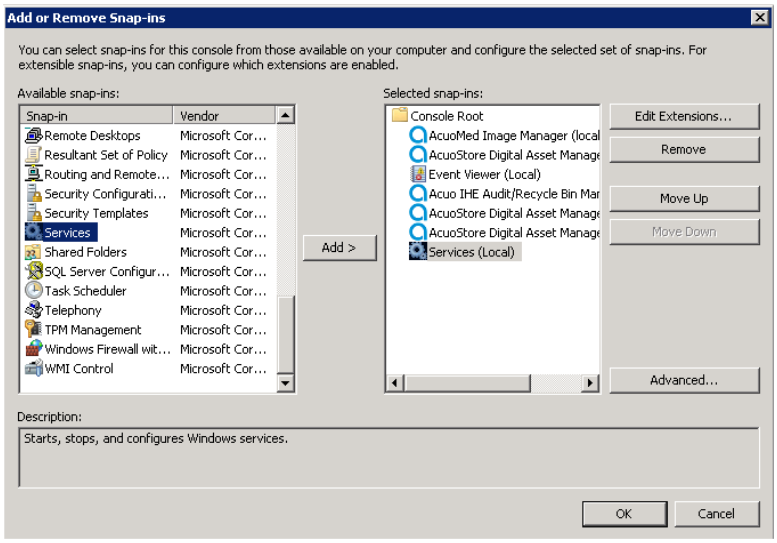


11. Click **Another Computer** to select it, click **Browse** to browse for another server, and, when you have selected the local server you want to manage, click **Finish**.

Note: When you click **Browse**, the Select Computer dialog displays, which is a standard Windows browsing window that lets you attach to any server on your Intranet or VPN connection. Alternatively, if

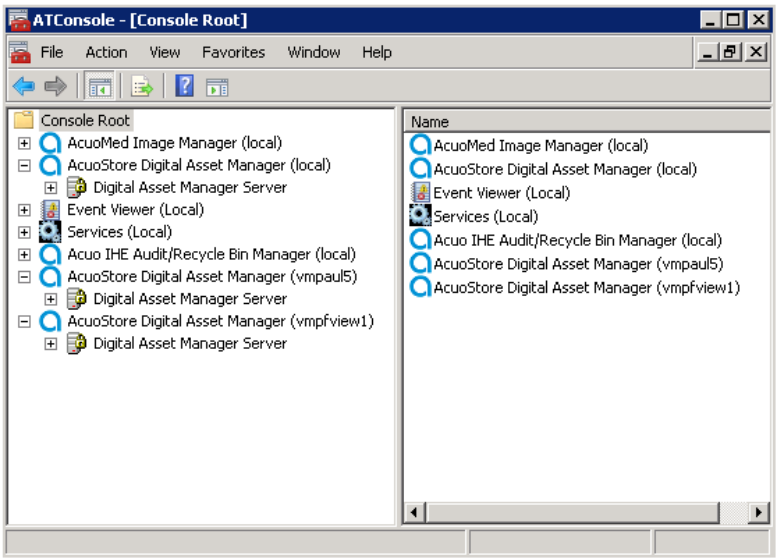
you know the name of the server that you want to connect to just type the name in the field provided, and then click **Finish**.

The Add/Remove Snap-in dialog displays.



12. Click **OK** to continue.

The Console Root screen displays.



13. From the Console menu, select **Save As** and save the new MMC console.

MMC Maintenance

With ongoing remote operations, there may be a time when you want to do certain tasks from a local server that has Windows on it but does not have AcuoMed or AcuoStore. If this is the case, one option is to only install the MMC console. Once this is done and you have set up the MMC console on the local server, you can manage MMC console services on remote (target) servers running Acuo products, provided you can gain secure access to the remote server via an Intranet or Internet VPN connection. Also refer to the topic *MMC Console Creation* on page 32.

Once you have set up a local system to manage MMC console applications on a remote system, there is little to do from a maintenance standpoint other than to carry out the tasks that are required to fulfill your business needs. However, the tasks you may perform are limited to those tasks that the MMC console applications manage on the remote system. By contrast, you can perform many more tasks via the Terminal Services Client (see the next topic).

Management via Terminal Services Client

The Terminal Services Client lets you convert the terminal of a local server (local PC) into a terminal that can be used to manage a remote server. This is achieved from the local server by entering the remote server's login ID and password into a Terminal Services Client interface that creates a link to the remote server. By doing this, you log into the remote server from a local location. Using Terminal Services Client on a local server to manage a remote server eliminates the need to physically be where the remote server is located in order to perform management tasks on it. (This is the same as management via MMC console discussing in the previous topics). However, unlike MMC console, a Terminal Services Client lets you perform many more tasks on the remote server from the local server because you are actually logged into the remote server.

With Terminal Services Client, since you are logged into the remote server, you can perform any task (including managing MMC console applications) that you could do if you were physically sitting at the remote server. Typically, these tasks include (but are not limited to):

- Changing the configuration on the remote server
- Stopping and restarting services on the remote server
- Building a set of management entities that you want to routinely manage on the remote server
- Checking and/or changing remote server settings including communications and storage options

Terminal Services Operational Considerations

The Terminal Services Client also allows you to manage remote server MMC Console applications. Terminal Services Client is strongly recommended if you need to access the remote server through an Internet firewall. From an operational standpoint, Terminal Services Client is flexible and effective; it provides a variety of options so that it can meet the requirements of many different configurations.

To help determine whether using Terminal Services Client is an appropriate method for you to remotely manage other systems, review Figure 10 and the explanations that accompany it.

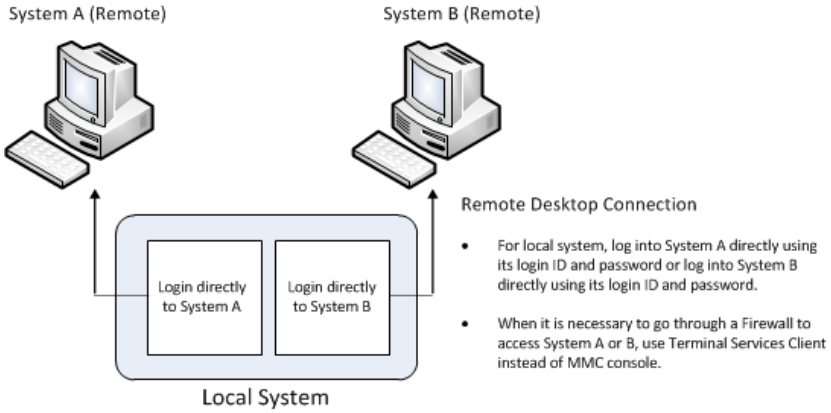


Figure 10: Remote management using Terminal Services Client

Figure 10 shows that from a local system that has a Terminal Services Client interface, you can log directly into a remote server by using its login ID and password. This is referred to as opening up a Terminal Services Client session. You may open up as many sessions as is practical.

In addition, Figure 10 notes that the Terminal Services Client method should be used if it is necessary to go through a firewall. This is because the Terminal Services Client uses a single TCP/IP port to gain access to the remote server.

Terminal Services Configuration

The following procedure describes how to set up a local server to manage Acuo services on a remote server using the Terminal Services Client.

NOTE: The following procedure assumes that the Terminal Services Client is running on your local server and that a Terminal Services Service is running on the remote server.

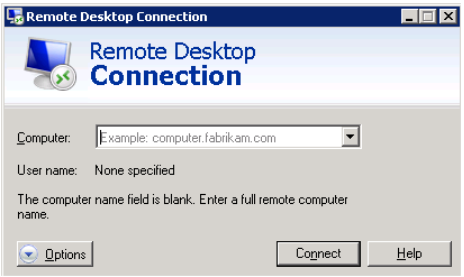
Furthermore, in order to complete this procedure, you must know the username and password of the remote server that you want to log into and manage.

1. Open the Terminal Services Client on your local server (via Start Menu→Run→MSTSC.

   The Terminal Services Client dialog displays.

2. From the Terminal Services Client dialog list of Available servers, highlight the name of the server you want to manage, and click **Connect**.

   The Log On to Windows dialog displays.

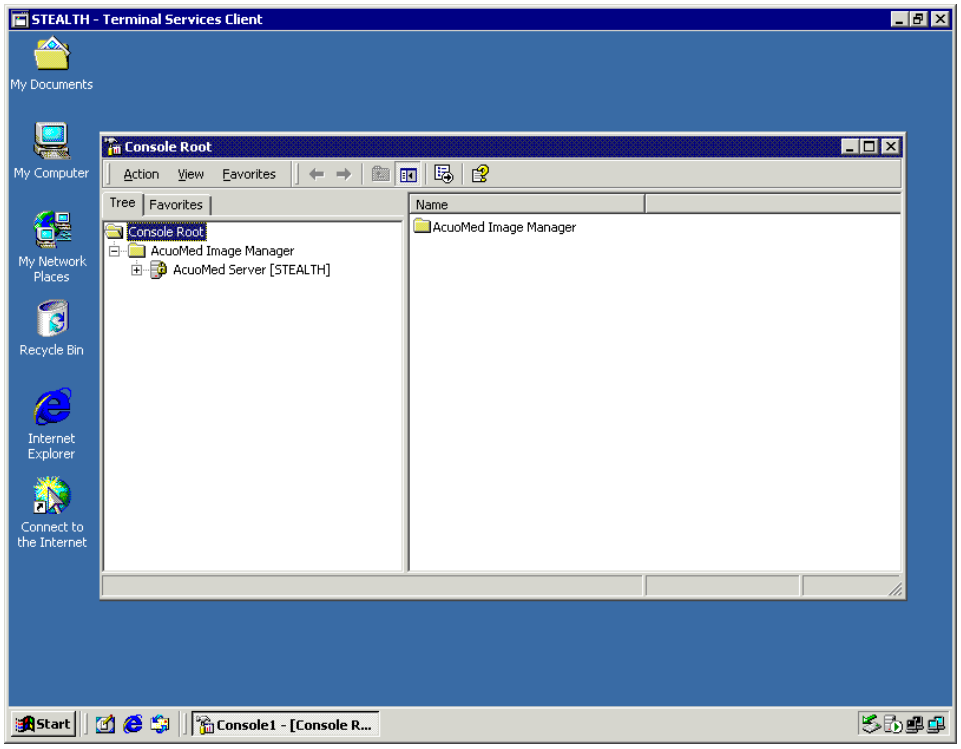


3. Enter the parameters for the server you want to manage.
    1. Type the computer name
    2. Type the User name
    3. Type the Password

    You are now ready to manage the remote (target) server.

4. On the target server you are remotely managing, open and use the applications needed to fulfill your business needs.

    The application interface of your choice displays.



Terminal Services Maintenance

Once you have set up a Terminal Services Client on a local server to manage a remote server there is little to do from a maintenance standpoint other than to carry out the tasks that are required to fulfill your business needs. Again, since you are actually logged into the remote server, you can perform any task on the remote server that you could do if you were physically sitting at the remote server.

Chapter 6 – System Backup and Recovery

In this chapter:

Overview

This chapter discusses the system backup and recovery considerations that users of Acuo Technologies' products should observe when making backup and recovery plans. The chapter is divided into two main topics:

- Backing up System Files and Databases
- Disaster Recovery Planning and Practice

The main goal of these topics is to help you, the Information Services Professional, integrate Acuo Technologies' products, and the images they are responsible for handling, into the system backup and recovery strategies and procedures you are already using for other mission-critical systems at your site. In other words, what is described below will give you the information necessary to handle Acuo Technologies' products safely and effectively, but it will not describe in a step-by-step manner how to perform the specific system backup and recovery procedures applicable at your site.

It is important not only that you have database maintenance processes and disaster recovery plans in place, but that you perform/practice these procedures on a regular basis.

NOTE: The following topics discuss AcuoStore system backup and recovery in the context of the Acuo Technologies client application AcuoMed. If you are using AcuoStore with a different client application, you will need to make the appropriate changes in the following procedures, according to the requirements of your client application.

However, while it does not describe how to perform system backups step-by-step, Acuo Technologies does recommend that when possible, you adopt the system backup principles outlined in at least one of the two configurations shown in Figure 11 and Figure 12.

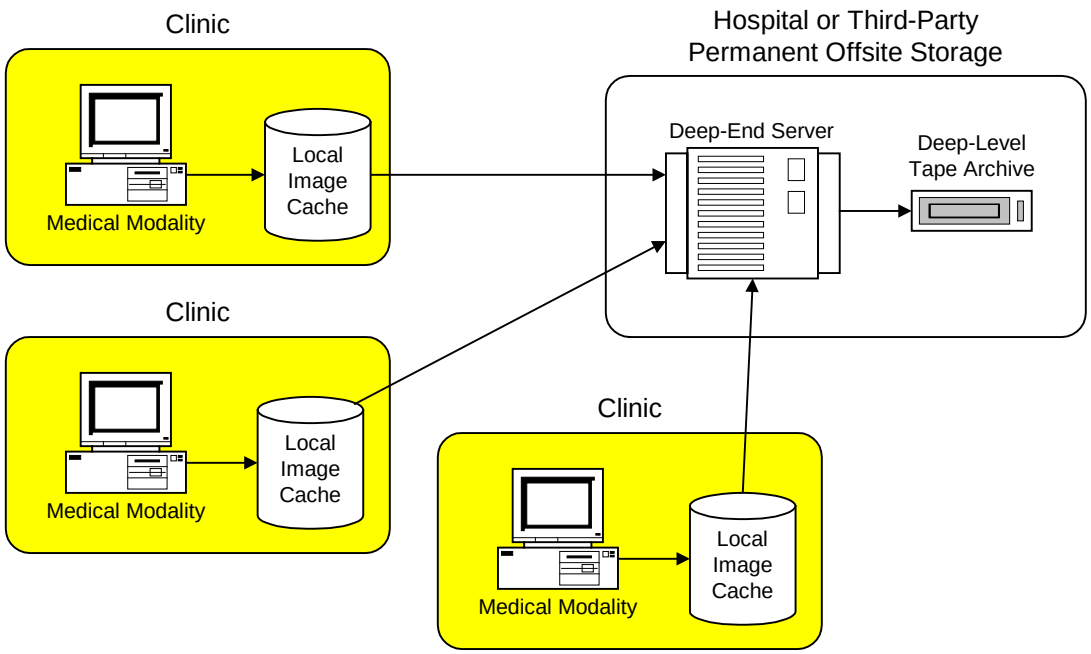


Figure 11: Temporal Server Model and Backups

Figure 11 shows a topology in which three clinics each have medical modalities and local image caches, but no deep-level tape archives. Instead, deep-level tape archive services are handled offsite at the centrally located, deep-end server. At the clinics, medical modalities save images to both the local image caches and the deep-end server at the same time. Later, in accordance with their temporal status, the local image caches prune (delete) images/studies after they have been stored for a preset amount of time. Finally, at the deep-end server, a complete set of all patients/studies/series/images is stored and incremental tape back-ups are conducted regularly.

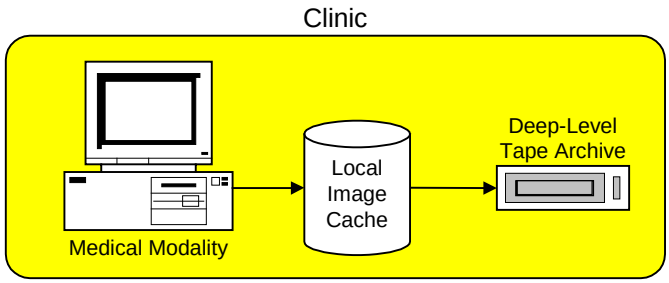


Figure 12: The Local Backup Archive

Figure 12, unlike Figure 11, shows that deep-level tape archive services can be handled onsite, or locally. In this scenario, care must be taken to ensure that incremental backups are conducted regularly as it is generally unlikely that this function will be handled automatically. In addition, it is often advisable to transport the tape backups to a secure, offsite location.

Lastly, note that the scenarios shown in Figure 11 and Figure 12 are only recommendations, and that in no way do they depict the only ways to handle system backups. On the contrary, your system and how you conduct backups will most likely vary. However, the common thread between both these scenarios is that for maximum security, Acuo Technologies recommends that you back up your images with a deep-level tape archive.

Backing up System Files and Databases

It is necessary to back up system files, databases, and assets:

- Windows and its system files including the Windows Registry file
- SQL databases and system log files
- HSM database (if using removable media through a third party HSM)
- Client application databases (for example AcuoMed DICOM database(s) and AcuoMed database)
- AcuoStore Database
- Digital asset files – backup all managed shares within AcuoStore

IMPORTANT: From the standpoint of Acuo Technologies' products, the key consideration to observe when backing up system files, databases, and image/digital asset files is the order in which you perform the backups. Refer to the procedure below for more information.

Backup order is critical to maintaining database integrity. To explain, when images come into the AcuoMed DICOM Database, the AcuoMed DICOM Database puts references to these assets into the AcuoStore Database automatically. So if the AcuoStore Database was being backed up before the AcuoMed DICOM Database and items arriving in the AcuoMed DICOM Database while the AcuoStore Database was being backed up, there could be references in the AcuoMed DICOM Database to assets that were not in the backed up version of the AcuoStore Database.

NOTE: The topic following this one, *Disaster Recovery Planning* and Practice describes how to plan for a disaster such as a fire or other type of catastrophic event. In that topic, you will find references indicating that part of planning for a disaster is to carry out, on a scheduled basis, the numbered steps that follow in this procedure, *Backing up System Files and Databases*.

When backing up Acuo Technologies' system and database-related files, do so in the following order:

1. Backup Windows and its system files, including the Windows Registry file.

   To do this, follow the procedures found in Microsoft documentation for backing up these files.

2. If you are using removable media technology, back up the HSM database.

3. Backup the SQL databases and system log files.

   To do this, refer to the separate topic *Recommended Acuo Maintenance Plan* on page 71.

4. Do an incremental backup of the image files.

   To do this, use standard backup procedures. An incremental backup of image files lets you only backup new image files rather than backing up all your image files each time you make a tape backup.

5. Backup the Acuo Technologies installation directory.

   This is the directory where you installed your Acuo software. To do the backup, use standard backup procedures.

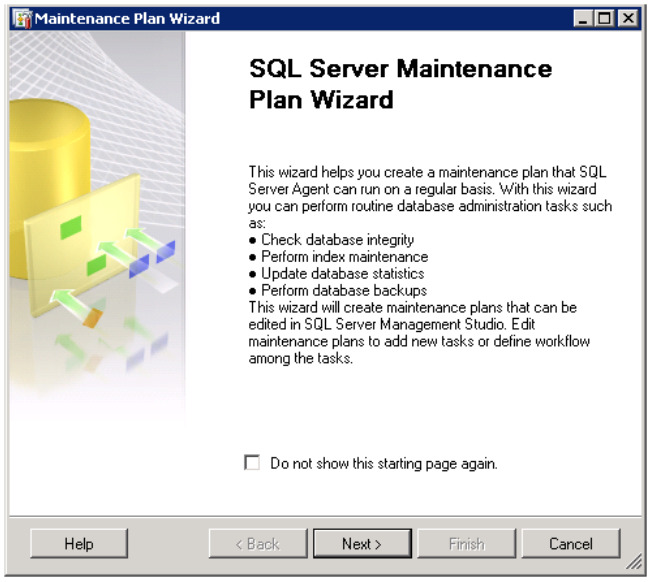
Recommended Acuo Maintenance Plan

The following maintenance plan setup is recommended for a Microsoft SQL Server environment.

AcuoMed and AcuoStore Database Backup Plans

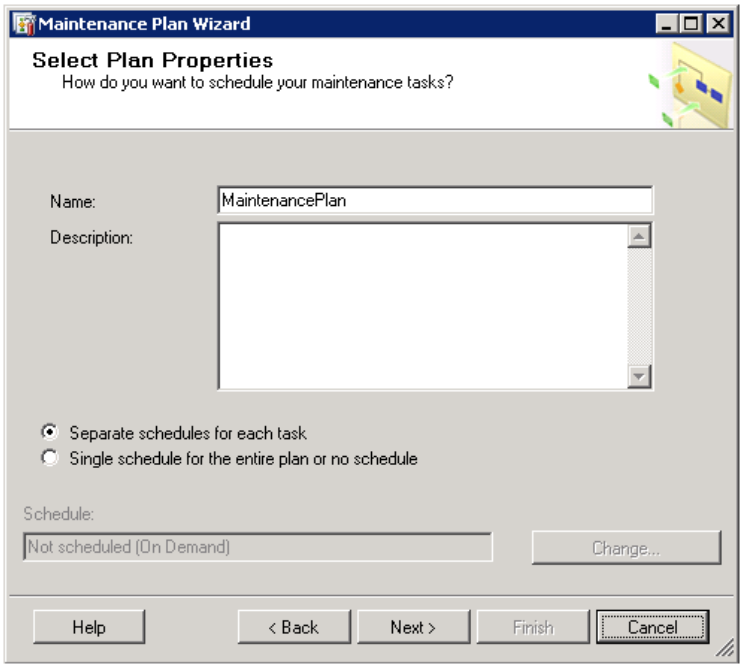
1. **Open "Enterprise Manager"**
   - Select <Start> <Programs> <Microsoft SQL Server> <SQL Server Management Studio>

2. **Create Acuo Database Maintenance Plan**
   - Select <Management> and <Maintenance Plan>
   - Right-click on <Maintenance Plans> and select <New Maintenance Plan…>
   - The "Welcome to the Database Maintenance Plan Wizard" window appears



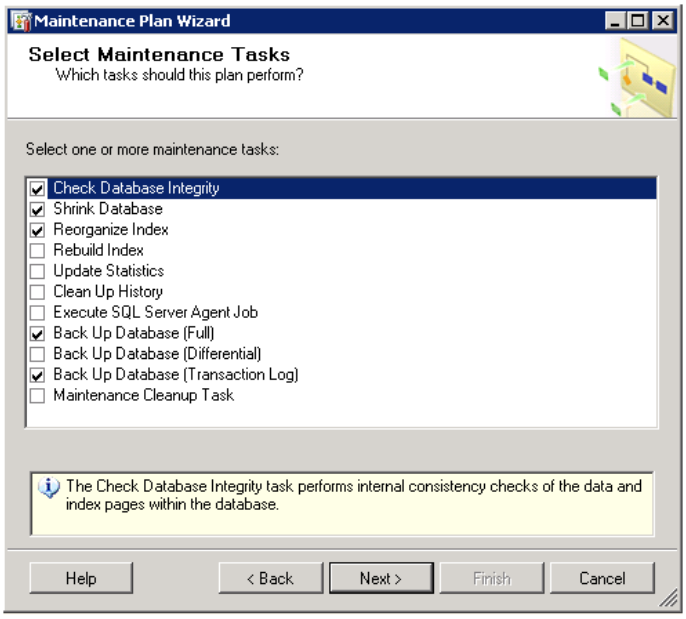
   - Select <Next>

- The “Select Plan Properties” window appears



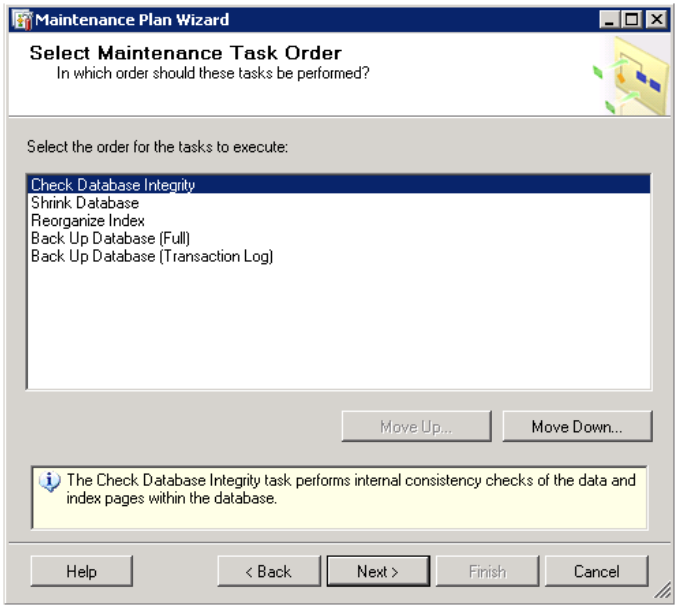
  - Provide Name and Description for Maintenance plan
  - Choose separate schedules for each task in the plan.
  - Select <Next>

- The “Select Maintenance Tasks” window appears



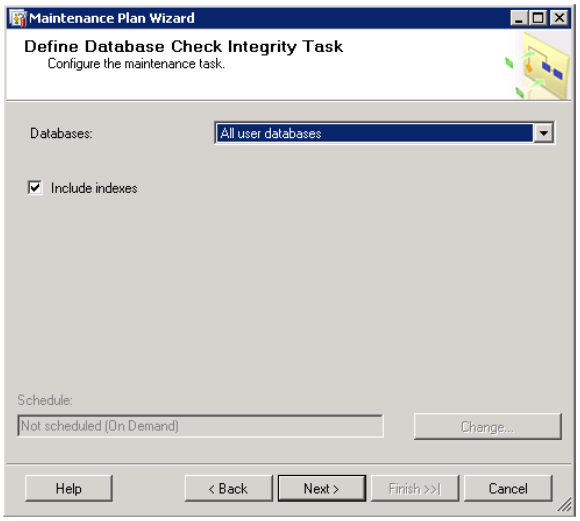
  - Select Shrink Database and Reorganize Database
  - Select <Next>

- The “Select Maintenance Task Order” window appears



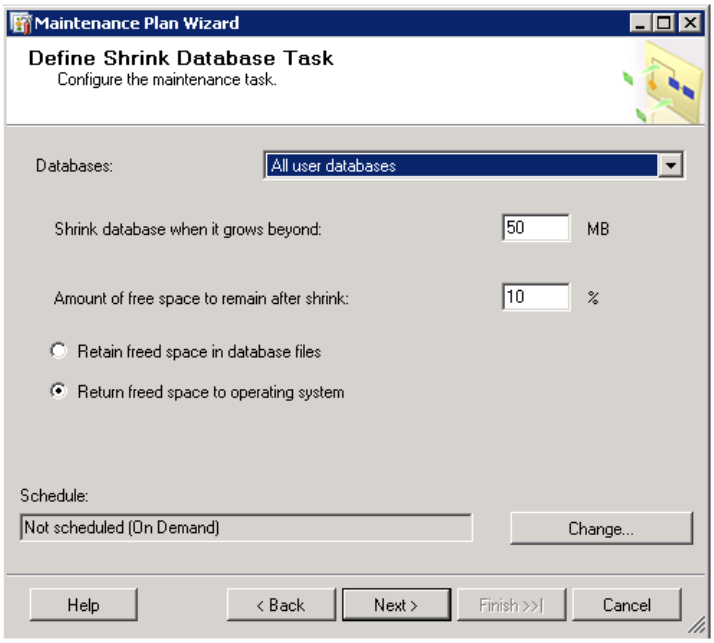
  - Select <Next>

- The “Define Database Integrity Task” window appears

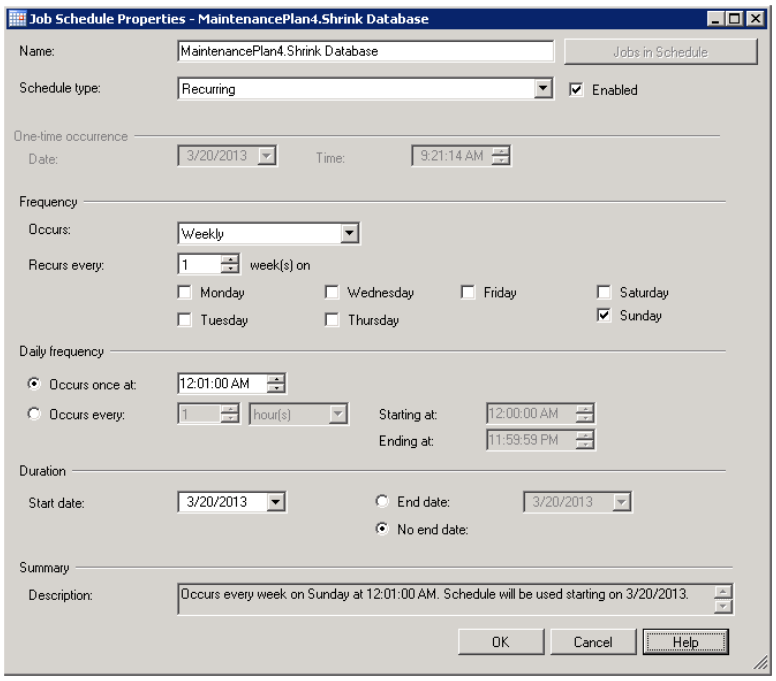


  - Select All user databases
  - Select <Next>

- The “Define Shrink Database Task” window appears

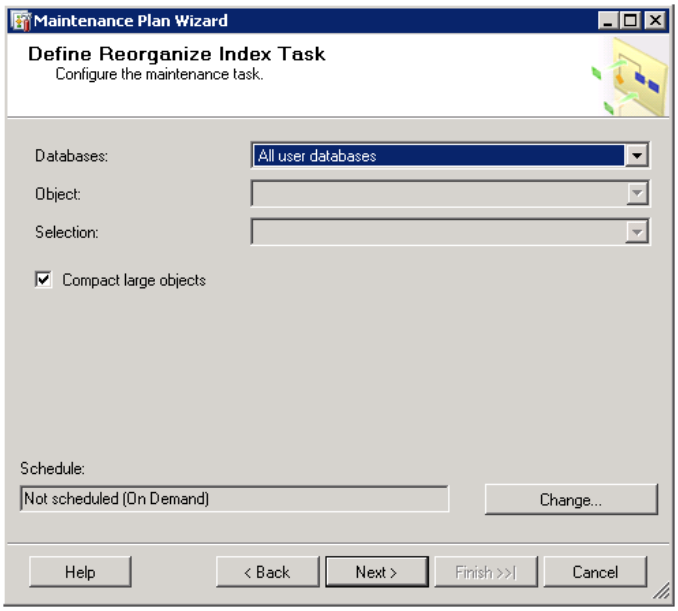


- Select All user databases
- “When it grows beyond” <50 MB>
- “Amount of free space to remain after shrink” <10%>
- Select <Change>

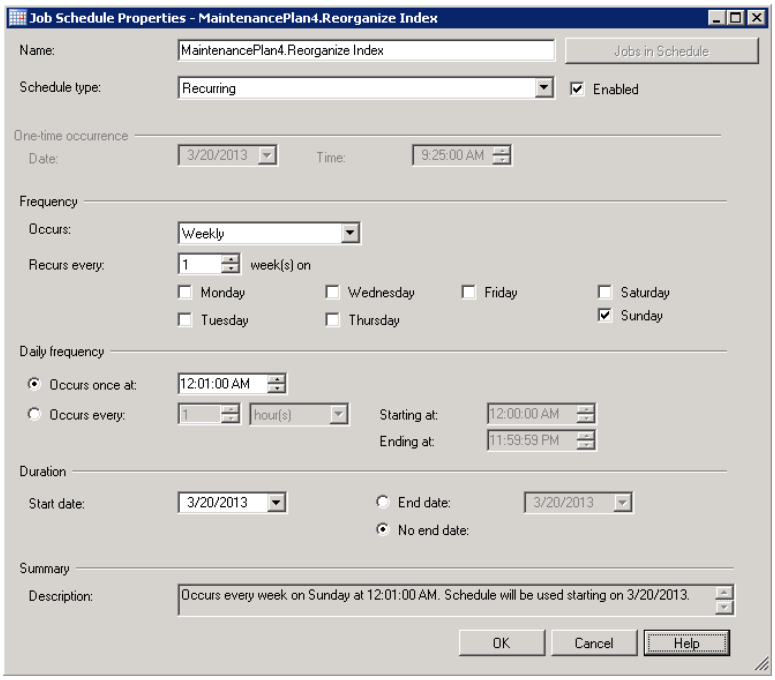


- Set Job Schedule Properties
- Select <OK>
- Select <Next>

- The “Define Reorganize Database Task” window appears.

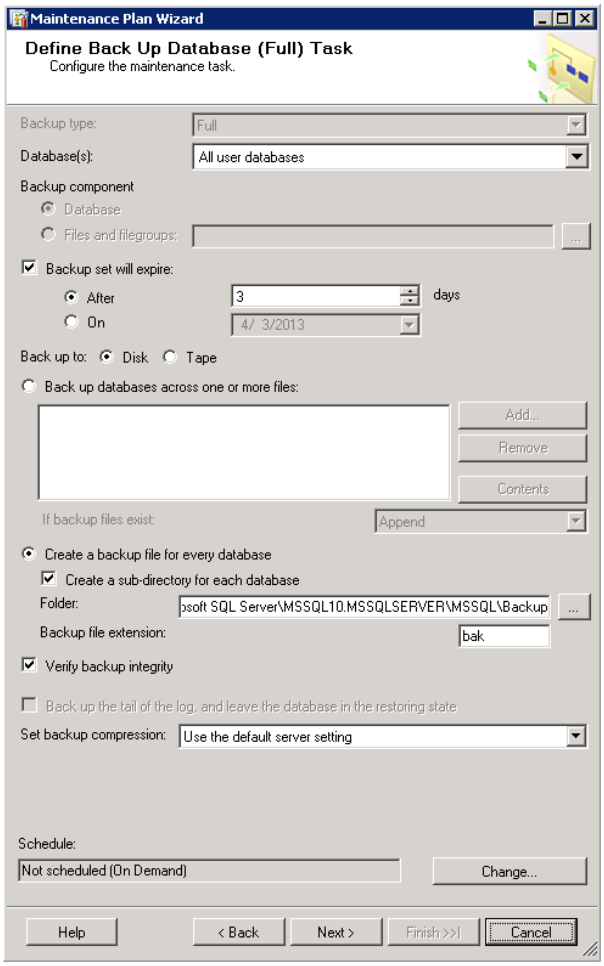


- Select All user databases
- Select <Change>



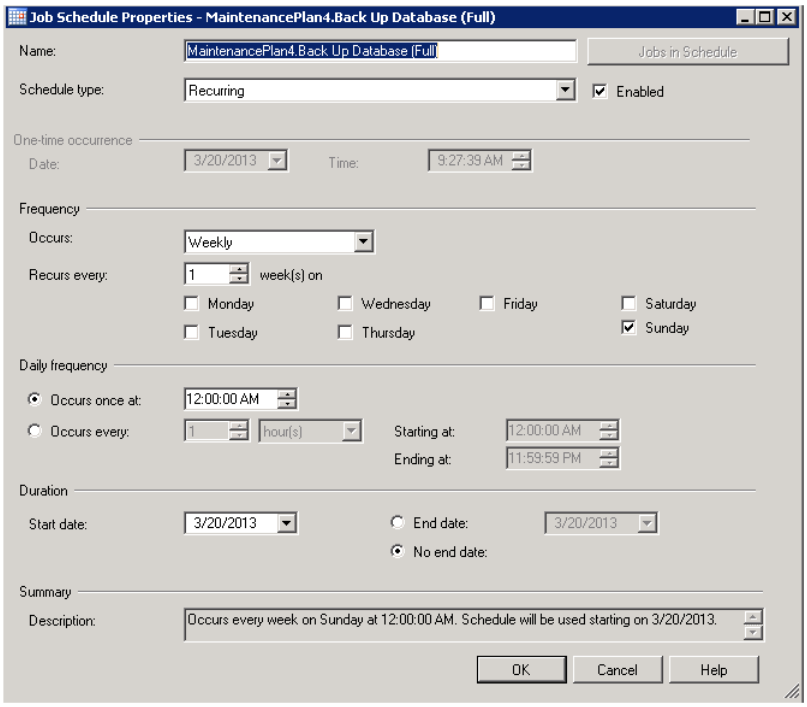
- Set Job Schedule Properties
- Select <OK>
- Select <Next>

- The “Define Back Up Database (Full) Task” window appears.



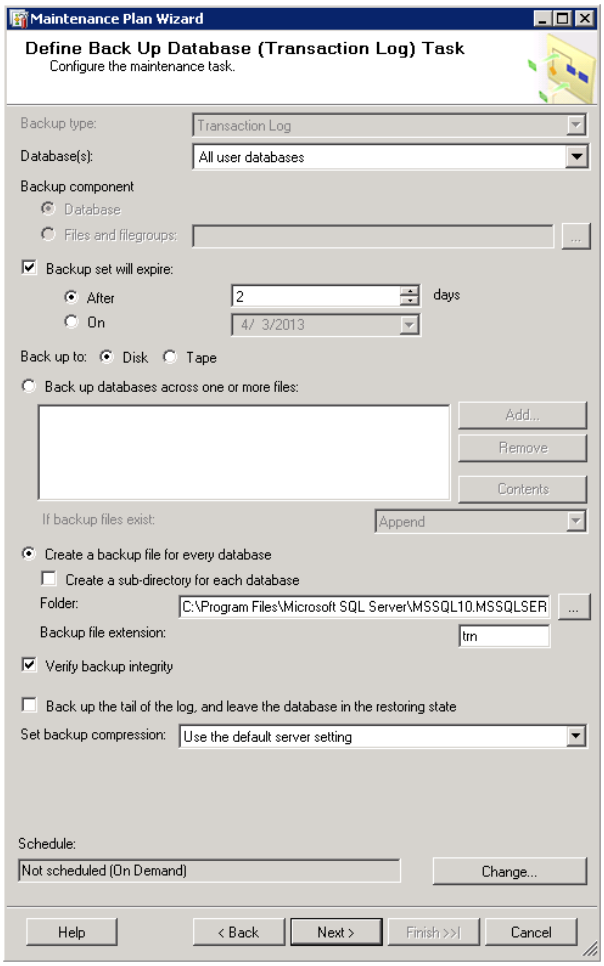
- Select All user databases
- Select Back up to “Disk” or “Tape”
- Choose location for backup files to be placed for each database.
  - Should be on different disk than OS
  - Should be on different disk than Databases and Transaction Logs
  - Should have 50 GB free space
- Check “Verify backup Integrity” (optional)
  - Positive – Increase the probability of a good database backup
  - Negative – Database backup time is doubled

- Select <Change>



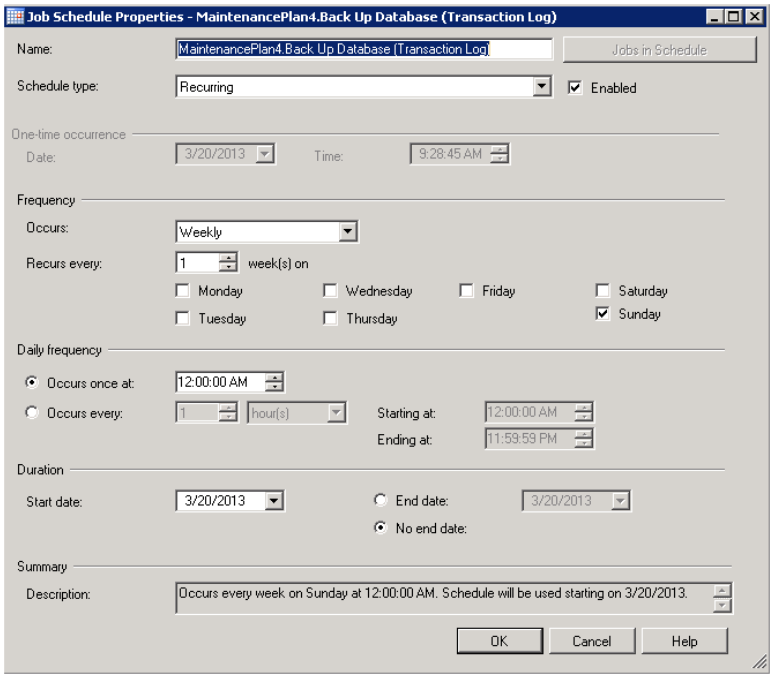
- Set Job Schedule Properties
- Select <OK>
- Select <Next>

- The “Define Back Up Database (Transaction Log) Task” window appears.



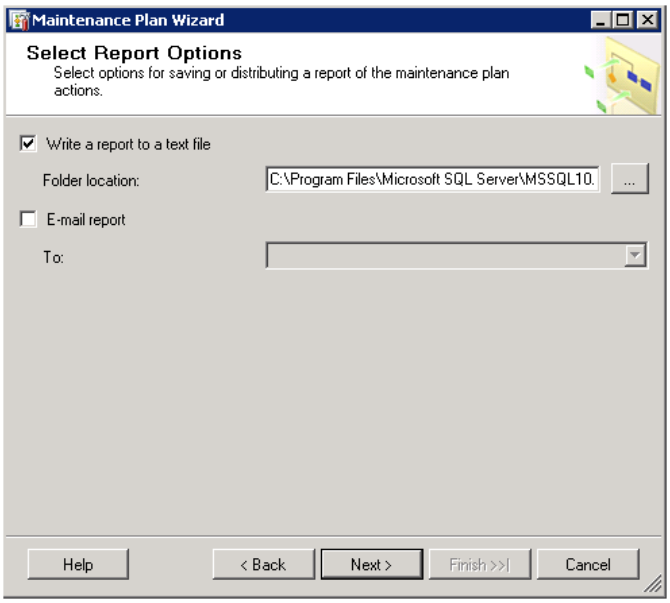
  - Select All user databases
  - Select Back up to “Disk” or “Tape”
  - Choose location for backup files to be placed for each database.
    - Select a location for the backup files
    - Should be on different disk than OS
    - Should be on different disk than Databases and Transaction Logs
    - Should have 50 GB free space
  - Select <Create a subdirectory for each database>
  - Check “Verify backup Integrity” (optional)
    - Positive – Increase the probability of a good database backup
    - Negative – Database backup time is doubled

  - Select <Change>



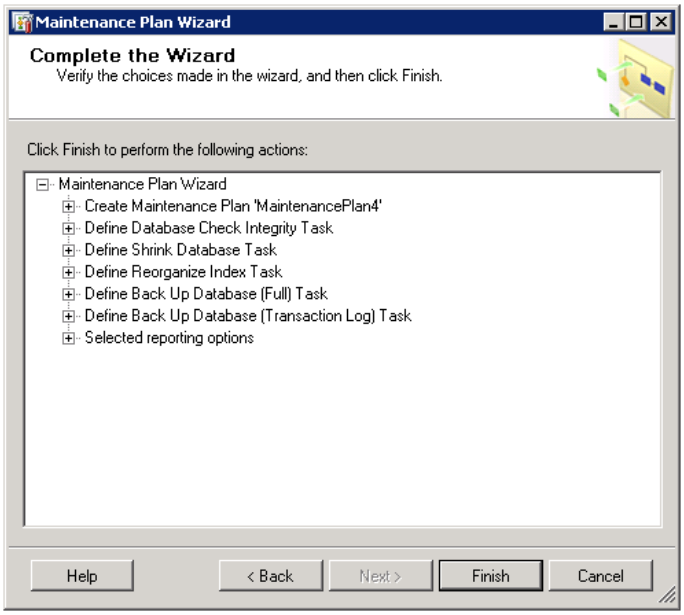
- Set Job Schedule Properties
- Select <OK>
- Select <Next>

- The "Select Report Options" window appears.



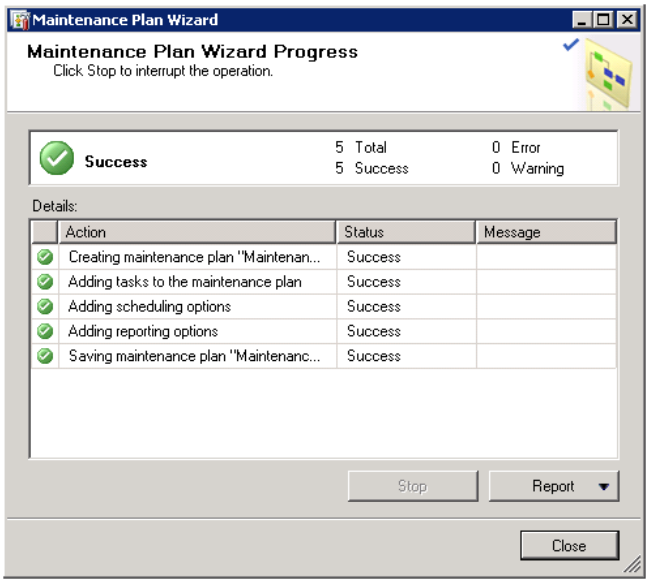
- Choose Folder Location
  - Should be on different disk than OS
  - Should be on different disk than Databases and Transaction Logs
  - Should have 50 GB free space
- Select <Next>

- The “Complete the Wizard” window appears



  - Select <Finish>

- The “Maintenance Plan Wizard Progress” window appears



  - Select <Close>

HSM Operations for Jukeboxes

It is recommended that you use the copying facilities of the HSM to create onsite and offsite backups of your digital assets. You can set up a job that automatically makes up to three copies of a tape:

- One copy remains in the tape jukebox
- One copy is ejected for onsite backup
- One copy is ejected for offsite backup

Refer to the appropriate HSM information for backup and recovery procedures.

Disaster Recovery Planning and Practice

If some type of catastrophic event should happen in which you lose data, you should have a Disaster Recovery Plan in place that lets you recover your mission-critical business data and resume operations as quickly as possible. Therefore, drafting such a plan should be a priority if you do not already have a plan in place. Otherwise, if you have already implemented a plan, you should now consider updating it to reflect the addition of your Acuo Technologies implementation.

IMPORTANT: It is critical that you not only have a disaster recovery plan, but that you practice it to ensure that all people involved knows their roles and that the plan is thoroughly tested and provides the required results.

First off, other than the order in which you should conduct backups as described in the previous topic, there are no particular things that you should consider with regard to disaster recovery planning that do not already apply to all Windows Server and most database applications. Therefore, Microsoft documentation on this subject, particularly topics in online help under *disaster recovery*, are applicable to your needs in this area.

However, so that you may have immediate access to disaster planning-related information, some key points for consideration are discussed below. These points should let you consider some of the more critical areas relative to Acuo Technologies' products. However, remember that these are just sample points. You must consider them on the basis of your own environment or in the context of your own recovery plans, and decide how to integrate them into your plans by modifying them accordingly.

Caution

The procedures that follow in this chapter are guidelines for implementing disaster recovery. Use these general guidelines as a starting point for drafting a detailed and comprehensive disaster recovery plan that applies to your site and overall business requirements.

General Planning Considerations

Generally, a Disaster Recovery Plan should include the following:

- How long will it take to recover data and, once this is done, what state can users expect data to be in? For example, the plan might state that recovery will take 24 hours and that users can expect no more than five days worth of data to be recovered and guaranteed.
- Who should be contacted in the event of a failure, and how should they be contacted (by phone, e-mail, pager, etc.)?
- Where should new hardware be obtained, if needed?
- Who is responsible for the plan?
- When was the plan last tested and how well did it perform? If there were failures during regular testing, or stress testing, were those failures addressed and, if so, were they re-tested? What were the results of those tests?
- Is management informed about the Disaster Recovery Plan and its specifications? Can stress and other kinds of testing substantiate the specifications?

Systems That Can Be Shut Down

To be prepared for a disaster, the following plan could apply to systems that you can shut down — that is, systems which do not need to operate continuously (24 hours a day).

1. Shut down your server, and complete all the steps noted in the previous topic, *Backing up System Files and Databases*.
2. Determine if there are functionality scripts that can be run to quickly find out if the system is functioning at minimal levels.
3. Consider performing database and transaction log backups during the day to minimize the amount of data you could loose during a day.

To recover data after some kind of disaster has happened, follow these steps:

1. Obtain suitable replacement hardware (if required).
2. Install your Windows operating system with appropriate service packs.
3. Install your SQL server software and its appropriate service packs.
4. Confirm that Windows and your server are operating properly.
5. Halt your server's operation.
6. Install your AcuoStore and AcuoMed systems in the same place you were originally running them.
7. Restore all Acuo databases to their original locations.
8. Start server operation.
9. Load any available transaction or database logs.
10. Run Consistency and Integrity checks on the databases.
11. Execute DBCC CHECKDB from query analyzer on all databases. This checks the allocation and structural integrity of all the objects in the specified database.
12. If you have a functionality script, run it to ensure that the system is running properly.
13. If all systems check out okay, allow users back onto the system.

Systems That Cannot Be Shut Down

To be prepared for a disaster, the following plan could apply to systems that you cannot shut down — that is, systems which operate continuously (7 days a week, 24 hours a day).

1. When you can, back up all transaction and system logs and databases to another computer, and to a deep-level tape archive.
2. Keep a record of where all your server and system files are located, as well as the service packs installed and any special database options.
3. If possible, create functionality scripts that let you quickly determine whether your databases are functioning properly without having to seek end-user verification.

To recover data after some kind of disaster has happened, follow these steps:

1. Obtain suitable replacement hardware (if required).
2. Install your Windows operating system with appropriate service packs.
3. Install your server software and its appropriate service packs.
4. Confirm that Windows and your server are operating properly.
5. Halt your server's operation.
6. Install your AcuoStore and AcuoMed systems in the same place you were originally running them.
7. Restore all Acuo databases and transaction logs from dumped files as appropriate.
8. Start server operation.
9. Load any other available transaction or database logs.
10. Run Consistency and Integrity checks on the databases.
11. Execute DBCC CHECKDB from query analyzer on all databases. This checks the allocation and structural integrity of all the objects in the specified database.
12. If you have a functionality script, run it to ensure that the system is running properly.
13. If all systems check out okay, allow users back onto the system.

Appendix A – Frequently Asked Questions

In this appendix:

General Questions

Here are a few frequently asked general questions about AcuoStore.

Am I limited in how much I can expand the physical storage that AcuoStore manages?

No. AcuoStore is extensible both within an individual AcuoStore Digital Asset Manager node and across your entire enterprise. You can expand the physical archiving space of individual AcuoStore Digital Asset Managers, add new AcuoStore Digital Asset Managers, and share resources and manage assets across a large, geographically-distributed AcuoStore network.

Do I need to do anything special when setting up RAIDs to work with AcuoStore?

It is critical that you initialize RAID storage that AcuoStore manages as dynamic disks to allow for volume spanning. The volume spanning facility enables AcuoStore managed shares to span more than one physical disk volume. This allows you to expand storage space by logically attaching a new physical storage device to an existing share.

NOTE: Windows 2000 cluster configurations require the use of Basic Disks.

For more information, refer to topics in Microsoft Windows Help regarding Dynamic Disks and Spanned Volumes.

Where can I get information on recommended configurations for AcuoStore?

Prior to installing AcuoStore, ensure that your hardware, software and network components meet or exceed the recommended configuration levels detailed in the *AcuoMed Image Manager Installation and Operations Guide*. Even if you are building an AcuoStore implementation with a client application other than AcuoMed, the recommended components that are described in the AcuoMed manual will prove very useful in terms of ensuring your implementation's overall success.

Installation Questions

Here are some common installation questions.

How do I know what hardware, software, and networking components I need for AcuoStore?

This information is provided in *Chapter 3* of the *AcuoMed Installation and Operations Guide*.

How do I estimate how much storage capacity I will need?

Refer to *Appendix C* of the *AcuoMed Installation and Operations Guide* which discusses how to use the automated tools that Acuo Technologies provides to assist you with planning your storage requirements.

Configuration Questions

Here are a few common questions relating to AcuoMed configuration. For each question, a general explanation is given of what you need to do. Also, a reference is given to one or more procedures that demonstrate how to perform the specific task. These procedures are part of the configuration example in Chapter 4. So, you can use them as a guide, but you will need to make changes (for example, IP addresses, route names, AE names, etc.) that are appropriate to your system configuration.

I made a configuration change, why am I not seeing it?

After you make changes to the AcuoStore configuration, you must restart the AcuoStore service in order for the changes to take effect.

For the specific procedure to do this, reference the topic Restarting the AcuoStore Services after Configuration on page 36.

How does AcuoStore connect to the physical storage space that it manages?

AcuoStore makes its connection to physical storage space by means of managed shares, which are its logical mappings to physical storage.

For general information on AcuoStore's use of managed shares, refer to *AcuoStore Architecture* on page 15. For the specific procedure to set up managed shares, reference the topic

How does AcuoStore control which subscribers have access to a managed share?

By means of applications, AcuoStore controls subscriber access to the managed share, or shares, that house the subscriber's digital assets. AcuoStore can allow multiple applications serving different subscribers to securely use the same managed share. In this way, applications are AcuoStore's way of allowing administrators to allocate specified amounts of storage to particular subscribers.

For general information on AcuoStore's use of applications, refer to *AcuoStore Architecture* on page 15. For the specific procedure to set up applications, reference the topic *Configuring Applications* on page 53.

What about other configuration options?

AcuoStore is flexible and can be set up in a number of configurations. If the items above do not address your configuration question, please review the information given in *Chapter 4 – AcuoStore Configuration Example*. If you still cannot locate the information you need, please contact Acuo Technologies for assistance.

Remote Management Questions

Here are some common remote management questions.

What are my options for remotely managing AcuoStore?

You can remotely manage AcuoStore Digital Asset Managers via either an MMC console interface or a terminal services client (terminal server) interface. Deciding which of these methods best fits your needs will depend on your system and network configurations and the extent of your remote management requirements.

For more information, refer to the topics *Management via MMC Console* on page 58 and *Management via Terminal Services Client* on page 65.

Can I manage multiple AcuoStore Servers and applications from a single MMC console?

Yes. You can add remote systems to a single local MMC console and manage an entire set of distributed AcuoStore resources from this single console. Or, if you find it more convenient, you can set up a separate MMC console on your local machine for each AcuoStore system you want to remotely manage.

For more information, refer to the topic *MMC Console Creation* on page 32.

Are my remote management sessions secure?

Yes. AcuoStore security is integrated with Windows logon security for MMC applications. And the terminal services client interface requires the same user authentication (user name and password logon) as is required to log on if you were actually at the remote system. It is recommended that if you are accessing remote systems across the Internet, that you do so across a virtual private network (VPN) connection that is secured by a reliable authentication means (such as SecureID token authentication).

System Backup and Recovery Questions

Here are some common backup/recovery questions.

What is the best way to create onsite and offsite tape backups?

It is recommended that you use a backup product you are comfortable with to create onsite and offsite backups. The backups and the restore process should be readily available and practiced in the event that a recovery would need to be performed.

Appendix B – Troubleshooting

In this appendix:

Overview

This appendix describes the various steps that you can take when you encounter problems using Acuo products. All Acuo products use log files in an attempt to output information about every possible type of problem that might occur. In the event that you encounter a problem, you should consult these logs first for possible causes.

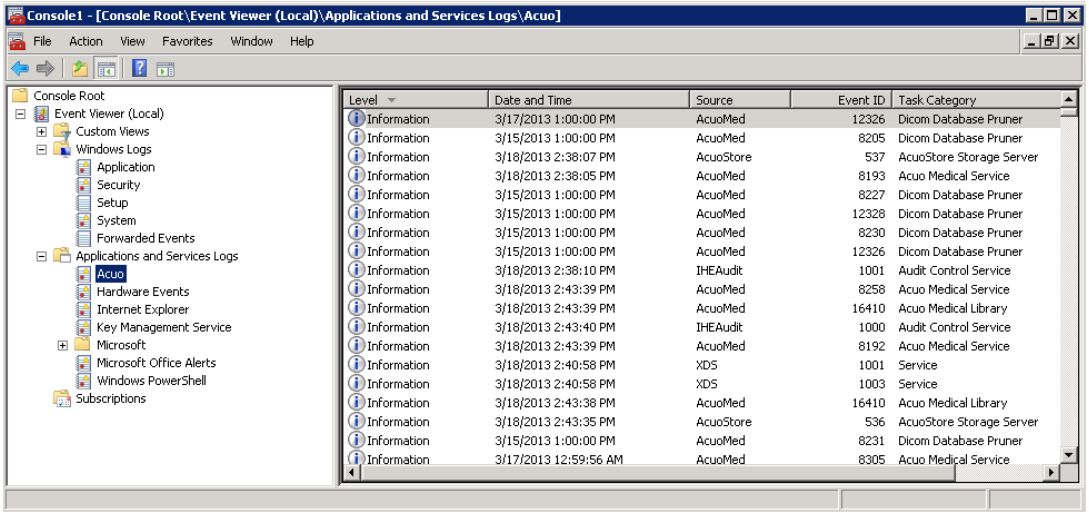
This appendix describes the following troubleshooting aids:

- **Event Viewer (Event Log)** – Lets you view four event logs to obtain problem information.
- **Trace Settings** – These monitors are part of the MMC console, and traces can be turned on at virtually every level of Acuo software to help determine a problem.
- **Third-Party Software** – These are non-Acuo programs that add other capabilities.

Event Viewer (Event Log)

The Event Viewer within Windows lets you view four event logs. Each of these logs runs constantly and, when you encounter a problem, you can open the Event Viewer and select from one of the four event logs to obtain more information.

To open the Event Viewer, from the Windows Start menu, select **Programs→Administrative Tools→ Event Viewer**.



The Event Viewer contains the following three event logs:

- **Application Log** – This log contains messages that describe events that are generated by Windows applications and services (including Acuo products). For information on how to view Acuo events only, see the next topic.
- **Security Log** – This log contains messages about any number of security-related events that you, as an administrator, can configure. For example, you may want to have an event message generated every time a particular file is accessed.
- **System Log** – This log contains messages generated by operating system events. For example, if something were to go wrong with your network card, or if a connectivity problem occurred, you would find messages related to these problems in this log. Also, informational messages note that system services were either started or stopped.
- **Acuo Log** – This log contains messages generated by the Acuo application.

Each event log (when it is configured and in use) generates the following three message types:

Information – Information messages provide information about non-critical events.

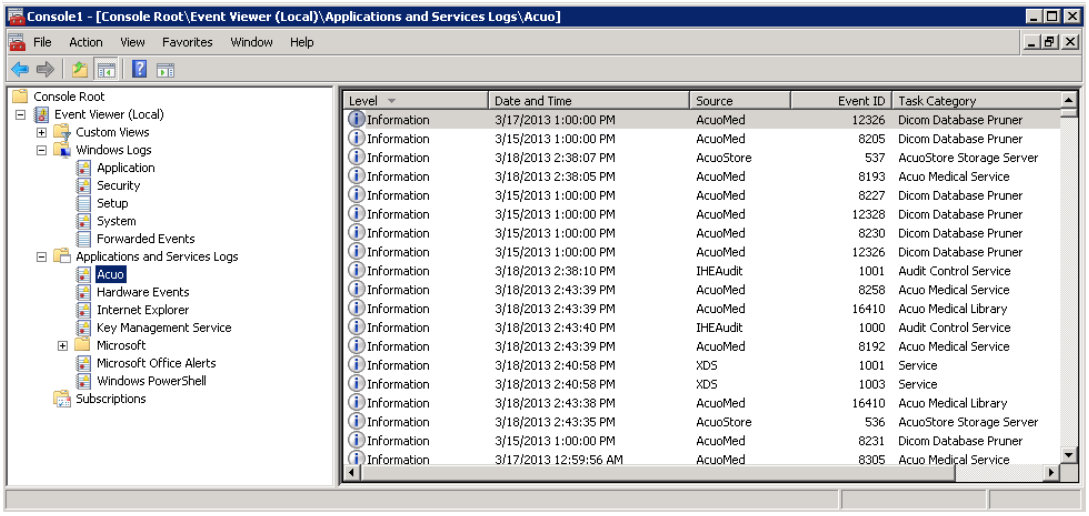
Warning – Warning messages usually indicate some kind of configuration error or network problem, or something that can be fixed by the administrator. Example warning messages include those indicating that the network or a database server is down or some type of configuration error is occurring.

Error – Error messages may require that you call Acuo Technologies to get assistance resolving the problem. First you can try stopping and restarting your services. If the problem persists after stopping and restarting your services, you should call Acuo Technologies for assistance.

NOTE: When using the Information, Warning, and Error messages to diagnose a problem, you should review several messages around a particular timeframe to gain a more comprehensive picture of what is happening.

Event Viewer

All Acuo event can be viewed from the within the Acuo application's MMC console tree. The source column indicates the source application.



Trace Settings

The trace setting monitors are part of the MMC console. Traces can be turned on at virtually every level of Acuo software to help determine a problem.

Caution

Trace Settings should be used with the assistance of Acuo Support staff. Please call Acuo Technologies before using any of the trace setting monitors shown below.

To access the trace setting monitors, follow these steps:

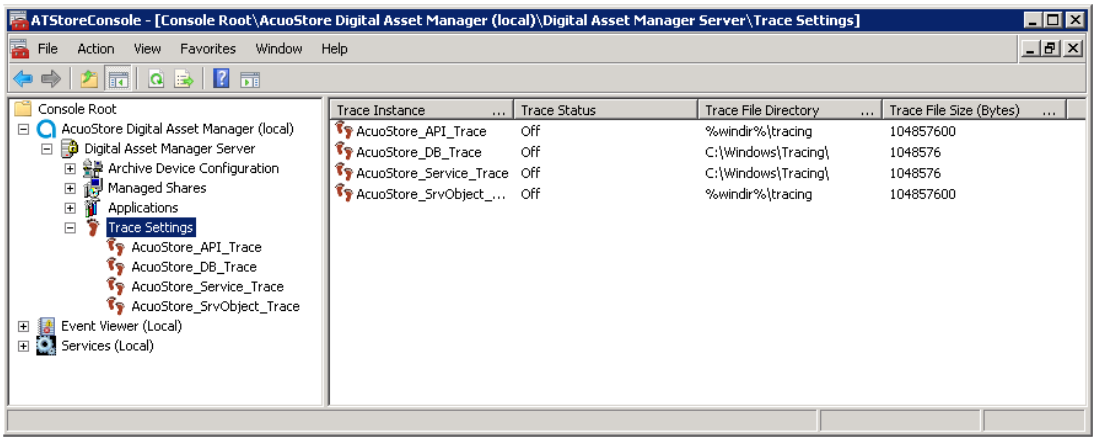
1. Start the Acuo MMC console, if it is not already running.

    1. Click the shortcut on the desktop

    The Acuo MMC console displays.

2. Expand the AcuoStore Digital Asset Manager until you can locate and open the Trace Settings folder as shown below.

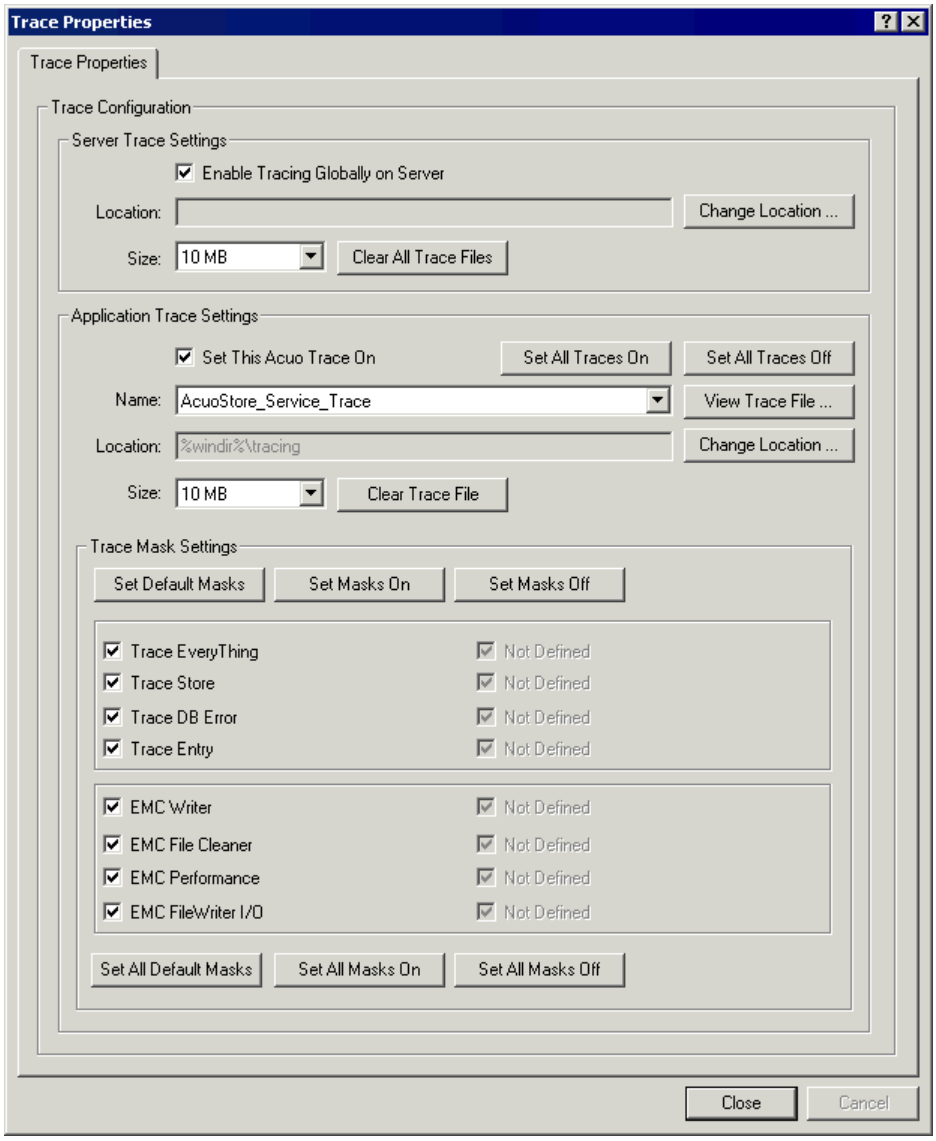
    All the available AcuoStore trace monitors display.



3. To activate a particular trace, right-click the trace you want to turn on and select **Set This Trace On** from the menu. This sets the trace to On with default settings.

   To activate a particular trace with specific settings, right-click the trace you want to turn on and select **Modify Trace Settings.**

   The Trace Properties dialog displays.

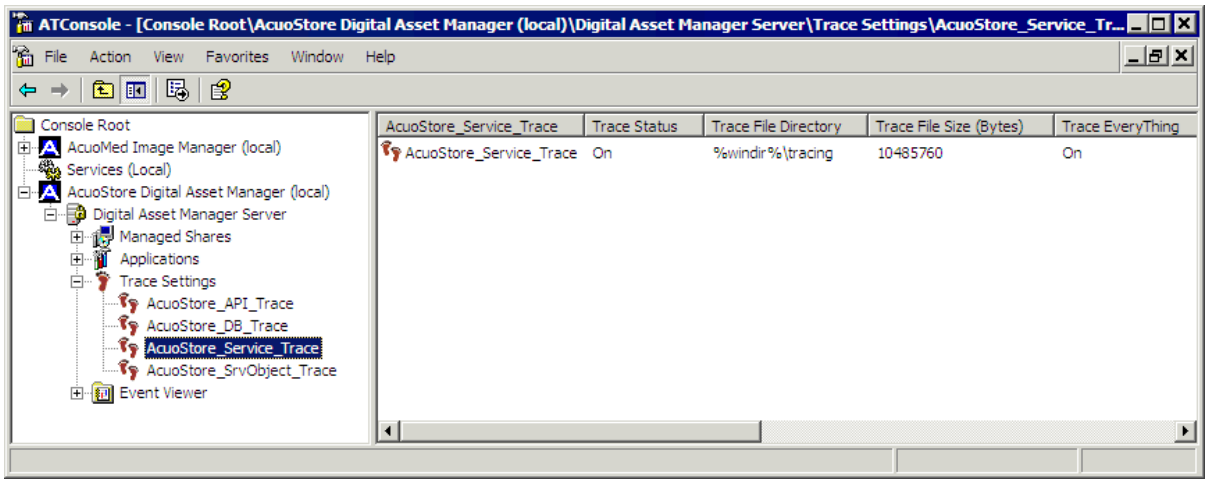


4. In the Trace Properties dialog set up the trace as needed. To activate the trace, be sure that the **Trace On** checkbox is checked.

   This dialog gives you much control over how the trace will behave. Most importantly, be sure to contact the Acuo Support staff about how to set up your traces.

5. Click **Close** to save your trace settings and exit.

   The trace you just activated will now show a Trace Status of **On** in the right window pane.



Note: By clicking the **Trace Settings** node, you can see a summary of which traces are On or Off.

Third-Party Software

Acuo recommends that you use some type of third-party, system-monitoring software to monitor the event log and other parts of your system. For example, certain third-party products can be set up to monitor the event log and page you or send an e-mail to you whenever a certain kind of event occurs.

The goal of using this type of software is to stay on top of your system and to minimize the possibility that data will be lost. Your system is made up of many very important components such as RAID storage devices, system drives, and databases. If any of these were to fail, you would want to know about it as soon as possible. It is practical to use third-party products to perform these monitoring tasks so that you can select the products that best fit your environment and system components. It is not possible for Acuo Technologies to anticipate every system configuration and all customer monitoring requirements. Therefore, using third-party software lets you supplement your Acuo systems environment with the tools that best suit your needs.

Appendix C – AcuoStore Network Profile

The following Network Profile for AcuoStore (and related services) should be used as a reference when planning or troubleshooting Anti-virus, firewall, VPN, load balancing or other network related technologies in conjunction with an AcuoMed or AcuoStore deployment.

Role	Protocol	Listening Ports
Server	TCP-DCOM (AcuoMed)	Dynamically assigned (135,1024-65535) *
Client	TCP/UDP-ADO (SQL Server)	
Client	TCP-CIFS	
Client	TCP-HTTP (Bycast)	
Client	TCP/UDP-Centera API	

Connection Usage Profile

Some client connections are managed in a pool, but most are dynamically requested and released as needed. The result on heavily loaded systems can be hundreds of connections per second being established or released, and thousands of open connections at a time. Some of this is mitigated or hidden by caching or pooling inherent to ADO & CIFS.

(*) DCOM assigns 1 listening port per server process, and relies on the Service Control Manager listening on TCP/UDP port 135 for DCOM port discovery. A more narrow range can be specified, though this is a server level specification, and Microsoft recommends a range of 100 or greater. Refer to the following documentation for more detail.

Using Distributed COM with Firewalls -- http://technet.microsoft.com/en-us/library/ff399341.aspx

How to configure RPC dynamic port allocation to work with firewalls -- http://support.microsoft.com/kb/154596

Glossary

This Glossary defines terms specific to Acuo Technologies' AcuoStore product and its operational environment. For the reader's convenience, some related general industry and computer terminology is also defined. Also, some basic AcuoMed terminology is included, since AcuoMed is used as the example AcuoStore client application in this document. For complete AcuoMed terminology definitions, refer to the glossary in the *AcuoMed Image Manager Installation and Operations Guide*.

AcuoMed Image Manager

AcuoMed Image Manager (AcuoMed for short) is Acuo Technologies' medical imaging product that provides an open-systems solution for transporting, storing, tracking, and retrieving digital medical images across an entire storage system network. When used generically, the term AcuoMed refers to the hardware and software system components that comprise Acuo Technologies' medical image and archive management product.

AcuoMed uses the AcuoStore Digital Asset Manager to manage physical storage and to store and retrieve digital medical images.

See also AcuoStore Digital Asset Manager.

AcuoStore Application

An AcuoStore application is used to configure which users(s) have access to which managed shares (according to username and password), and how much physical disk space will be allocated to each user. In this way AcuoStore applications make the linkage from client applications/users to logical and physical storage resources.

See also Managed Share.

AcuoStore Database

Contains information related to the bulk storage of digital images and related data including information about the shares and about the applications that use those shares.

AcuoStore Digital Asset Manager

The AcuoStore Digital Asset Manager is a general-purpose, digital asset retrieval service that lets you store, track, and retrieve virtually any type of digital asset routed to an AcuoStore archive from a client application such as AcuoMed.

See also AcuoStore Service and AcuoMed Image Manager.

AcuoStore Service

AcuoStore runs as a service within Windows and can be managed the same as other Windows Services via the Administrative Tools menu.

See also Service.

Acuo Tier Manager Service

This service is responsible for orchestrating the writing of assets to offline storage devices (EMC Centera excluded).

BLOB

Binary Large Object – an arbitrary set of bytes that may be an image, file, document or other object to be stored.

See also Digital Asset.

CAS Device

Content-Addressable Store, also referred to as associative storage or abbreviated CAS, is a mechanism for storing information that can be retrieved based on its content, not its storage location.

Client application

An application, for example AcuoMed, that manages and routes digital assets to a storage archive such as AcuoStore. For users who want to access an archive managed by AcuoStore with their own client application, an API can be provided that allows them to access AcuoStore.

Console

A console is an administrative structure that can contain tools, folders, Web pages, and other administrative items. You can set up different consoles to manage different parts of your AcuoMed/AcuoStore network (for example, a local console and a remote console). Consoles are hosted within MMC.

See also MMC.

Data Archive

For AcuoStore, this refers to a bulk storage facility for storing images and other data. This facility has no knowledge of DICOM; it keeps track of data BLOBs using globally unique IDs (GUIDs). The data archive has the ability to group data BLOBs into folders.

Data Storage Archive

The data storage archive stores and retrieves digital assets based on a GUID (Globally Unique ID).

Deep-Level Archive

A storage device such as a tape jukebox that is connected to a deep-end server to provide long-term archival storage of digital assets for one or more other network-connected devices. A deep-level archive is typically connected to a deep-end AcuoMed Server and is used to maintain a permanent DICOM archive.

DFS

Distributed File System – refers to a file system that simplifies the steps needed to use files located at various places across a network. Files can be drawn seamlessly from different parts of a network making it possible to have storage resources on different servers appear to users as one storage resource.

See also Logical Share (Managed Share).

DICOM

Digital Imaging and Communications in Medicine – The DICOM standard is a detailed specification for transferring medical images and related information between computers. DICOM is an open-systems standard that allows connectivity and interoperation of equipment from multiple vendors.

AcuoMed supports the DICOM 3.0 2000 standard.

Digital Asset

A digital asset is an image, file, document or any other combination of bytes that needs to be stored. (Some documents refer to this as a Binary Large OBject, or BLOB).

See also BLOB.

Find

The ability to locate an image (digital asset) that is stored on the AcuoMed network. Find represents the query portion of a retrieve request.

See also Move and Store.

Folder

A grouping of data assets that can be treated as a unit.

GUID

Globally Unique ID – The GUID identifies each specific digital asset for tracking and future retrieval. AcuoStore uses GUIDs to locate digital assets and make them locally available to requesters.

HIPAA

Health Insurance Portability and Accountability Act of 1996 - Security regulations published on August 12, 1998.

HIS/RIS

Hospital Information System/Radiology Information System – Medical administration systems that are used to manage patient information, track patient records, and schedule studies to be performed on modalities.

HSM	Hierarchical Storage Management – An application used for controlling and managing data storage across hierarchical layers of interoperating storage devices having different speeds and capacities. HSM enables data to be managed and stored on an appropriate medium according to its aging and anticipated retrieval requirements; this includes migrating data between storage devices when appropriate. HSM is a generic concept that includes many different vendors' storage system implementations (for example Microsoft's RSS and RSM products).
Local Image Cache	This is a DICOM temporal archive that is implemented on a temporal (department) server. The local image cache is typically a locally attached RAID that is used to store images that are associated with a DICOM database that is also located on the temporal server.
Local Server	In a remote management context, the local server is the system that you are using to manage another target system at a remote location. For remote management discussions, the local server is also referred to as the "local system" or "source system." See also Remote Server.
Logical Share (Managed Share)	A logical share, as opposed to a physical share on a local volume, makes it possible to extend a physical volume extensively by logically adding more physical volumes to the logically shared volume. For example, if you created a logical share to a 10-gigabyte physical volume and called that share Anderson_Images, the managed share, Anderson_Images, would have 10 gigabytes. However, since it is a logical share, you could attach another 10 gigabytes, or more, to the initial volume and the managed share Anderson_Images would grow to 20 gigabytes from 10 gigabytes. See also DFS and Physical Share.
Managed Share	A managed share is a logical mapping to a physical storage space. Managed shares are configured in AcuoStore. Once configured, managed shares function as a route through which digital images travel. There can be single or multiple managed shares going to one storage device. See also AcuoStore Application.
MMC	Microsoft Management Console – MMC is a framework for hosting administrative tools called consoles within the Windows 2000 environment. MMC provides the tools and commands that you need to build new consoles. See also Console.

Modality

Refers to a wide range of medical imaging devices that AcuoMed is capable of communicating with and receiving digital images from. Modalities include such devices as MRIs, CT Scanners, X-Ray devices, Ultrasound devices, etc. Basically, AcuoMed can interface with any modality that is DICOM 3.0 compliant.

Move

The ability to move an image (digital asset) from one place to another on the AcuoMed network. This includes the ability to route a retrieve request to more than one destination.

See also Find and Store.

Namespace

A namespace is a reference to a logical storage location in which multiple physical storage devices may be defined and accessed. For example, imagine that you have two computers shared on a network as *Computer X* and *Computer Y*. The name *Computer X* and the name *Computer Y* each become namespaces that are logical storage locations within which you have a physical C:\ drive. When selecting the C:\ drive, you must ensure that you are in the correct namespace, *Computer X* or *Computer Y*, to be assured of finding the data for which you are looking. Lastly, remember that within a namespace, you may add virtually any number of physical devices, thus expanding almost indefinitely the amount of space a namespace may represent.

Nearline Storage

When using a CAS Device, Nearline data is on the local cache and a copy also exists on the CAS Device.

NTFS

NT File System – a file system that you can select when you set up a computer running Microsoft Windows 2000. In contrast to the FAT or FAT32 file systems, an NT File System supports much larger volumes, and unlike the other file systems, and NTFS volume supports domains.

Offline Storage

When using a CAS Device, Offline is data that has been deleted/purged from the local cache and only remains on the CAS Device.

Online Storage

When using a CAS Device, Online means the data only resides on the local cache, and no copy exists on the CASE Device (if configured).

Physical Share (Local Volume)

A physical share is analogous to the physical C:\ drive on your computer. That is, a physical share can only be as large as the local drive actually is (for example, 10 GB). Since a physical share by definition is not logical, it cannot be expanded seamlessly the way a logical share can.

See also Logical Share.

RAID

Redundant Array of Independent Disks – A data storage method in which data is distributed between two or more hard disk drives in order to improve performance, reliability, and fault tolerance. Different levels of RAID (such as RAID3 and RAID5) offer tradeoffs regarding their access speed, reliability, and cost. For this reason, Acuo Technologies recommends different RAID levels for different system uses.

Remote Server

In a remote management context, the remote server is the system that you are remotely managing from another source system at a "local" location. For remote management discussions, the remote server is also referred to as the "remote system" or "target system."

See also Local Server.

RSM

Removable Storage Manager – A service included with Microsoft Windows 2000, RSM facilitates management of and communication among groups of libraries, disk drives, applications, and removable media. RSM enables multiple applications to share local robotic media libraries and tape or disk drives, and manages removable media within a single-server system. A group of libraries, drives, and media that are managed by RSM is called an RSM system. RSM also operates in conjunction with RSS to manage storage resources.

See also RSS.

RSS

Remote Storage Service – This Microsoft service monitors drives, and based on aging algorithms, moves files out to a tape. In addition, RSS also provides facilities for duplicating tapes for disaster recovery purposes. For RSS to manage a drive, the drive must be NTFS capable. RSS also operates in conjunction with RSM to manage storage resources.

See also RSM.

Service

A service is a program, routine, or process that supports other programs running in a Windows environment by performing a specific system function. AcuoMed and AcuoStore run as services within Windows and can be managed the same as other Windows Services via the Administrative Tools menu.

Snap-in

A snap-in is a type of tool that can be added to a console. Both the AcuoStore and AcuoMed applications are snap-ins that can be added to an MMC-supported console.

See also Console and MMC.

Store

The ability to save an image (digital asset) received from a modality to another DICOM device on the AcuoMed network. This includes the ability to save an image to more than one destination in a single operation.

See also Find and Move.

Subscriber

An individual medical professional, user, or remote clinic or hospital that has access to an AcuoStore-managed storage archive or device. Subscribers have a Subscriber ID that lets them access only their assets. Subscribers may have access to multiple archives or just one.

Terminal Server

See Terminal Services Client.

Terminal Services Client

A software application that lets you log into another computer via a TCP/IP port. In contrast to an MMC console remote management configuration, which lets you "talk" only to MMC consoles on other computers, a terminal services client lets you manage any part of another computer because you are actually logged into the remote computer.

Index

F

G

H

I

L

M

N

O

P

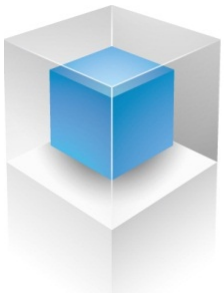
R

S

T

U

W



Acuo Technologies
Riverview Office Tower
8009 34th Avenue South.
Suite 900
Bloomington, MN 55425 U.S.A.

www.acuotech.com