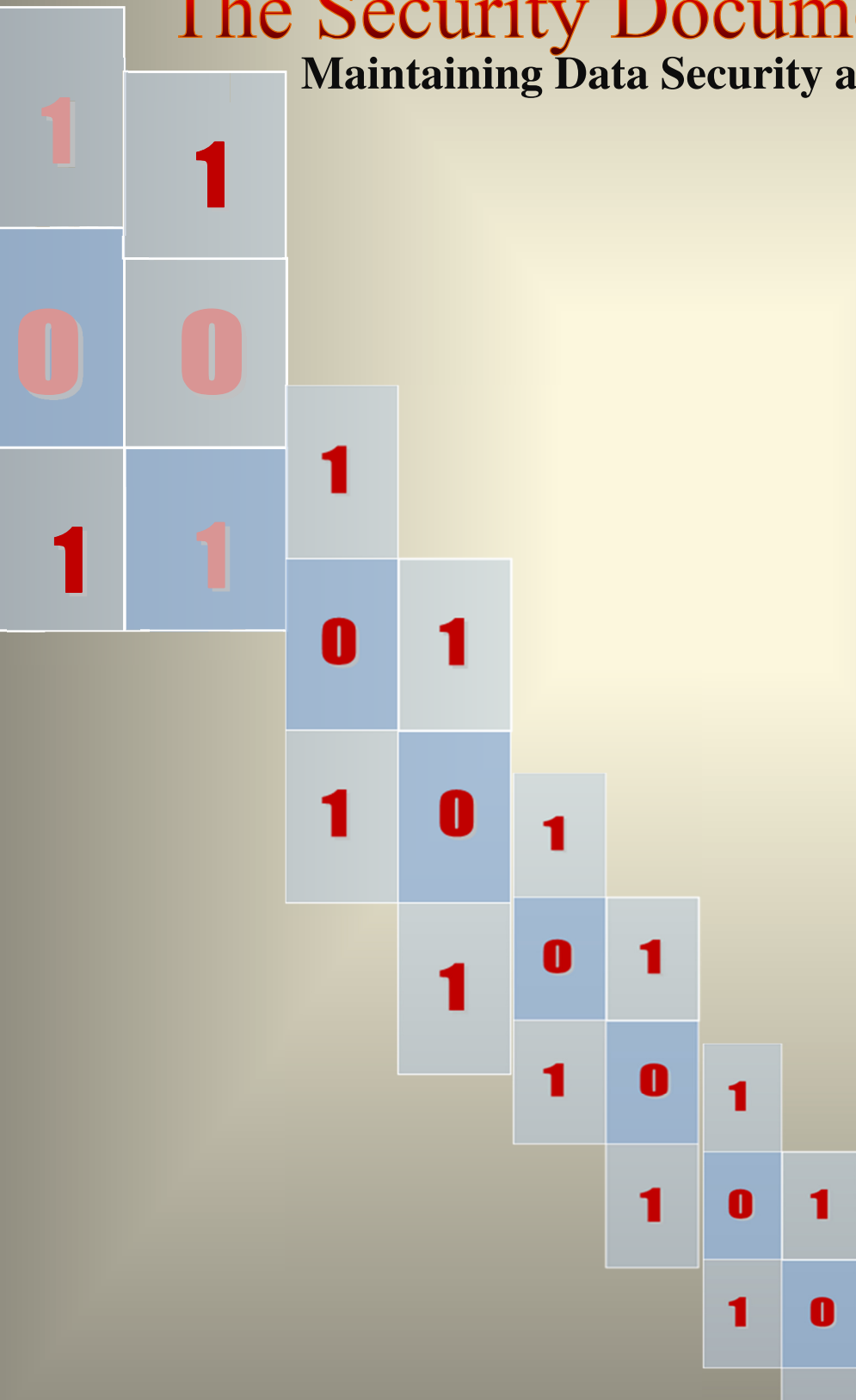




# The Security Document

Maintaining Data Security and Integrity



There are many aspects relating to data security and patient confidentiality. There is the network security- both external and internal, software accessibility, and component accessibility within the software itself. Here is the best way to address an applications level of vulnerability.

By analyzing the application and the interactions of the end user, we have identified the most vulnerable points of threat. Identifying and defining the vulnerabilities has allowed us to develop “onboard” tools for protecting and safeguarding the applications data. In this case the applications data is Personal Health Information (PHI).

The points of vulnerability are listed below.

- 1) Application Accessibility
- 2) Record Accessibility
- 3) Data in Transit - Transmission between the Client and the Server
- 4) Server Vulnerability
- 5) Data Backup

The following pages will better define the database utility and the tools there in. This will include how these tools are applied to protect and maintain the database.

## Data Risk Management

Data risk management is accomplished through the use of a database utility application and other tools that are native to the application. These tools are used to not only protect and maintain the database, but also to accomplish the tasks of backing up and recovering data. No third party software is needed for the security of the data that resides within the AudBase Database. The database engine of AudBase includes a self-analyzing process that will identify many forms of possible data corruption. For example, data fields and indexes have checksums, and when AudBase detects potential data corruption, it records information about the record in a special area of the data file, which is used when running the AudBase (4D) Tools application. These built-in automatic functions result in a real-world database that rarely experiences corruption or a need to be rebuilt.

Recourse is carried out through the use of continually running log files. These files log or record every action performed on the database by the clients and every transaction between the AudBase server and other servers / applications (EMR). Much like the Windows System Restore function, these logs can be used to restore (rollback) the data file to an earlier point in time.

Risk levels are addressed by these tools and safeguards. In many cases, the risk level is nulled or, at the very least, significantly minimized. The application has safeguard tools that minimize risk are intended to be employed jointly with the institution's overall system protection. Since part of the data risk management equation rests on the institution's Standards and Policies we can assume that the safeguards provided by AudBase, along with the institution's system integrity, will be adequate in securing PHI.

## Identified Risks

### Application Accessibility

As with any application, the ease in which a user can gain access to the database or execute the program is a risk. The level of risk is based on the contents of the database, the applications level of importance, or control to the overall system. Since PHI makes up the bulk of the data being stored within the AudBase database and the AudBase executable directs this data, accessibility rights are taken very seriously.

### Tools available for Database and Application Protection

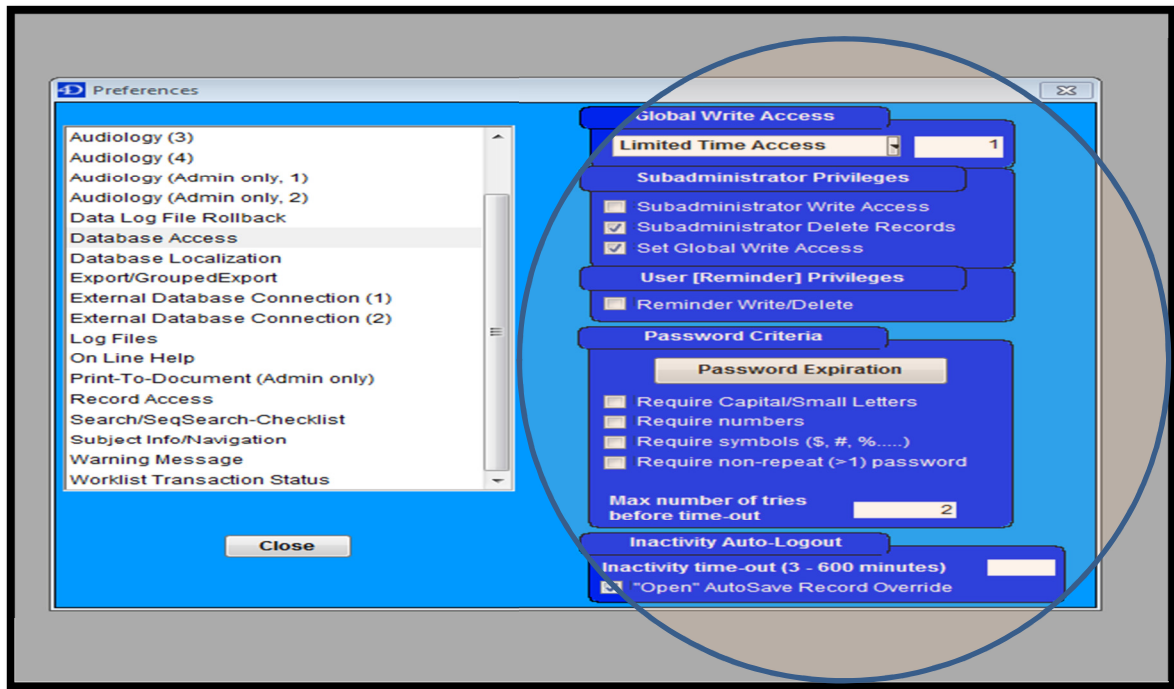
AudBase incorporates a comprehensive password access system. The password system is used to selectively grant read/write, read only, non-access, anonymity access, or even limited time access to users for any part of the database. Depending on your site's requirements, access can be granted, or denied, to input screens, view screens, report generation, schedule making, (PHI) etc. For example, if you have volunteers, you can provide access to certain administration files, but deny access to the actual patient medical records, thereby maintaining patient confidentiality. The extent of this kind of protection at the user level is so flexible that it can be used to even deny a user access to a button action that may be present on a form.

### Password Security and Recovery

All user-assigned passwords including the Administrator password are encrypted at rest and stored in the database. The passwords are stored in data segments that have no read accessibility and are not accessible to the end users. The administrator can only access the password data segments. The administrator is given a special "encryption and extraction" password which allows for the extraction of a password/s from the data segments. Once the Administrator logs in using the encryption password and selects the data file used, a double encrypted extraction file is created. Both the password and the extraction file are encrypted. This file created must be sent to AudSoft for unlocking and rendering.

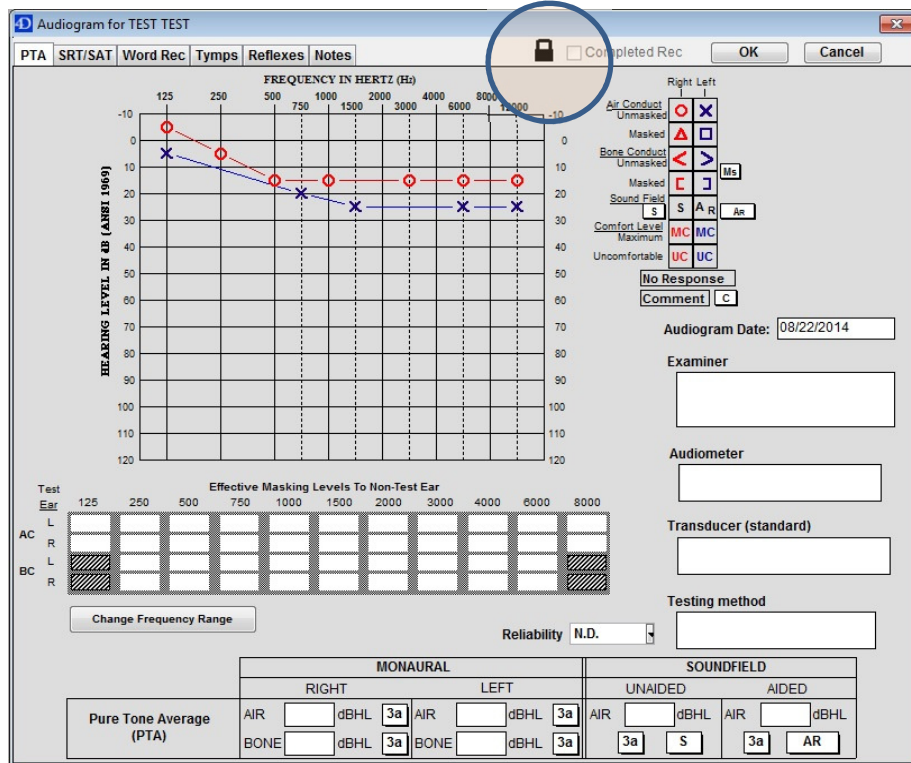
This guarantees that there must be two parties participating in the extraction process, both the owners of the database and an AudSoft representative to decipher a password.

Below is an example of the access control levels and the password complexity levels.



## Record Accessibility

When you call up a previously saved data-entry form (see screen shot below), it starts out “locked” in Read Only mode. This allows more than one person to access a record at the same time, and also prevents changes to the record. Even in a single-user environment, it is important to load records by default in Read Only mode because the typical record should not be changed after it has been saved. This is crucial for data integrity in any database or long-term clinical study.



- 1) **Black, closed lock:** The form is locked, but can be unlocked by clicking the icon.
- 2) **Black, open lock:** The form is unlocked.
- 3) **Red, closed lock:** The form is locked, and you cannot unlock it. This lock is commonly used by the application to lock down any record / encounter within AudBase that has been transmitted to a third Party software or database. This prevents an altered encounter from being resent without the knowledge of the Administrator.



If a user tries to unlock a form while another already has the form unlocked, an alert dialog box will pop open. The form will still be available to view in locked mode. The AudBase administrator can “unlock” any record and, if needed, grant other users this privilege.

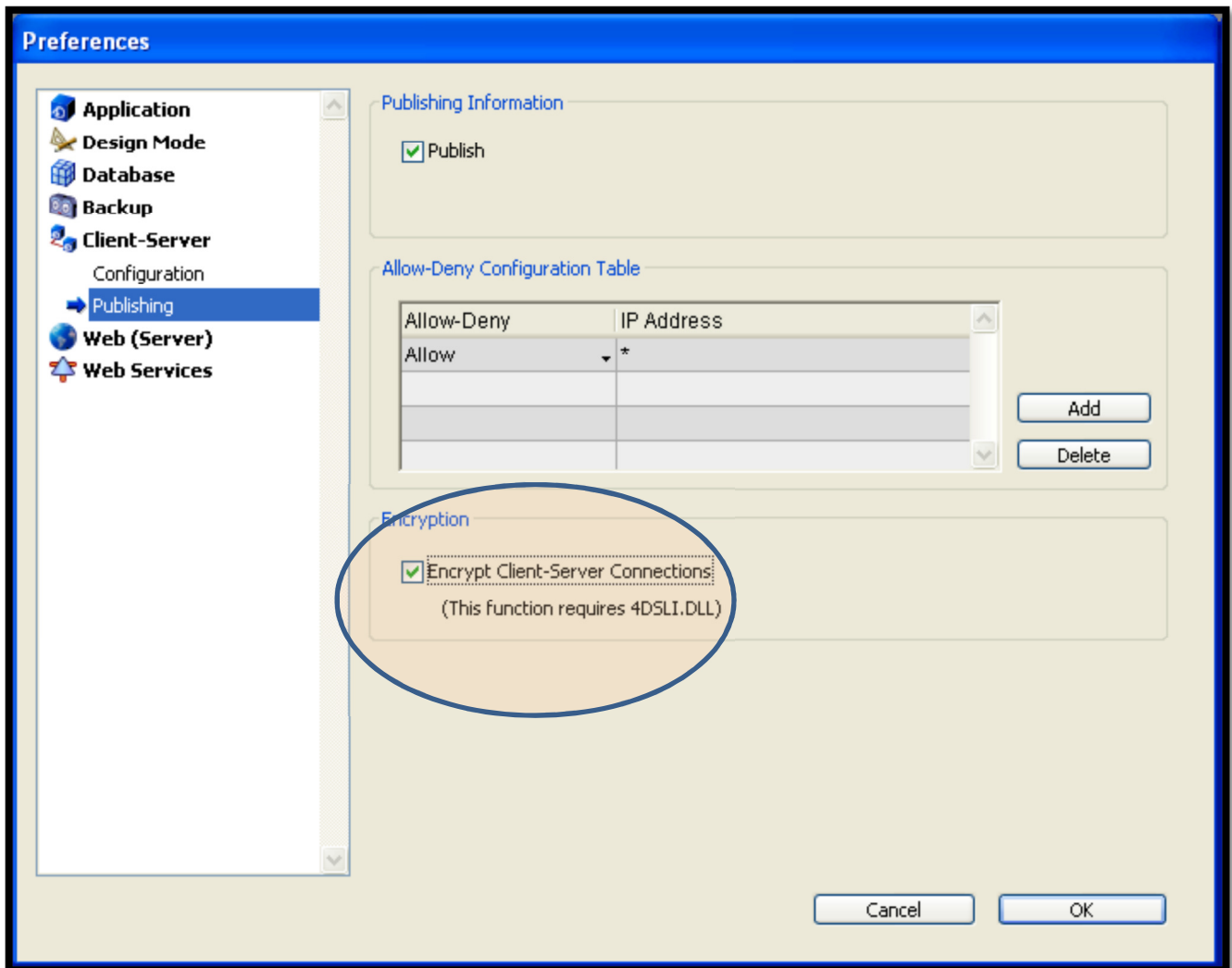
This feature protects the database from the tampering of a recorded or stored record and only allows for an Administrator or properly assigned users to unlock the record.

### Data in Transit - Transmission between the Client and the Server

The AudBase database is as secure, if not more secure, than other software on your network. This is true because of the program's own sophisticated security system. With a secure network, access to the information within the database is protected from external access. The database's password system and built-in encryption and decryption package using 128 SSL add an additional level to the existing network security system. In fact, a significant difference in 4th Dimension to other database engines such as MS Access is the ability to use SSL encryption and authentication between AudBase (4D) Client and AudBase (4D) Server. This feature insures that information passing between the user and the database is not intercepted nor altered by internal or external forces. When the web publishing interface is used the same level of security provided by secured bank web sites is available.

Another security feature, AudBase is coded to make use of local workstation cache. By employing the strategy of caching settings and benign information (non PHI) locally we can limit the transaction traffic between the client and the server to a minimum.

Below is an example of how easily it is, within the server console, to enable encryption between client and server.

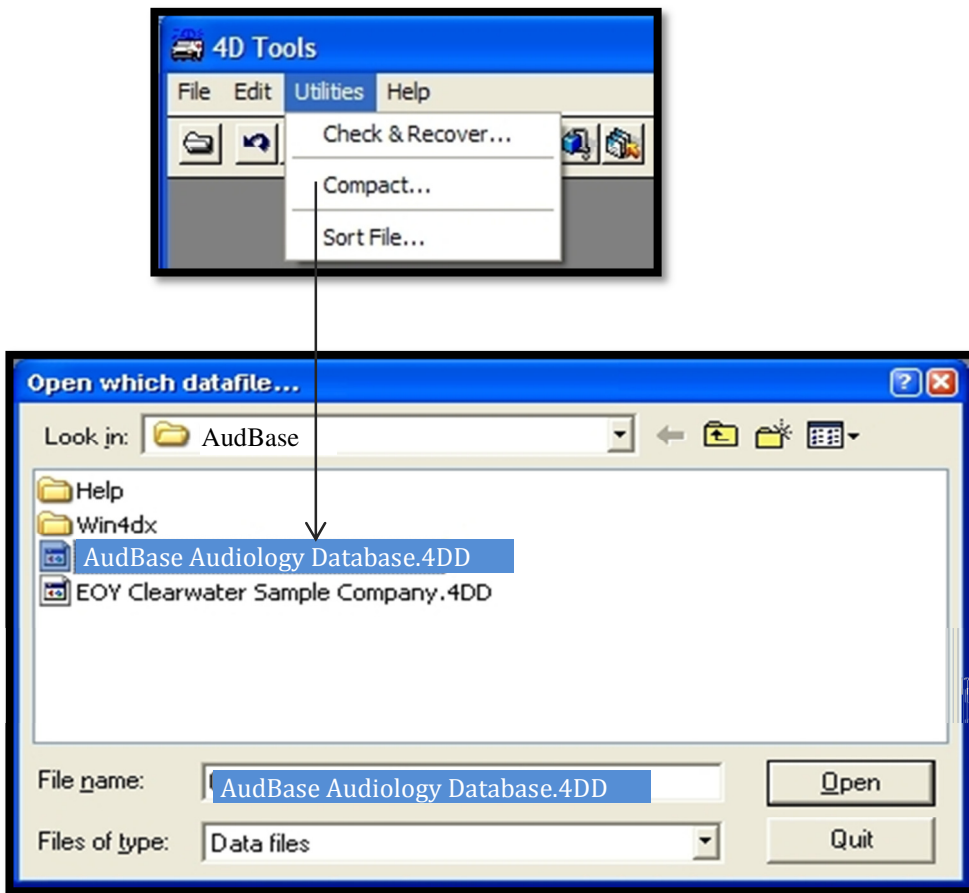


## Server Vulnerability - Data Protection and Database Maintenance

Though the server is password protected and within the institution’s firewall, it is still vulnerable to corrupted data. Upon database failure or mal-operation there are options for rectification. 4D tools is a database maintenance utility that can be run against the database either for ongoing maintenance or for database repair and recovery.

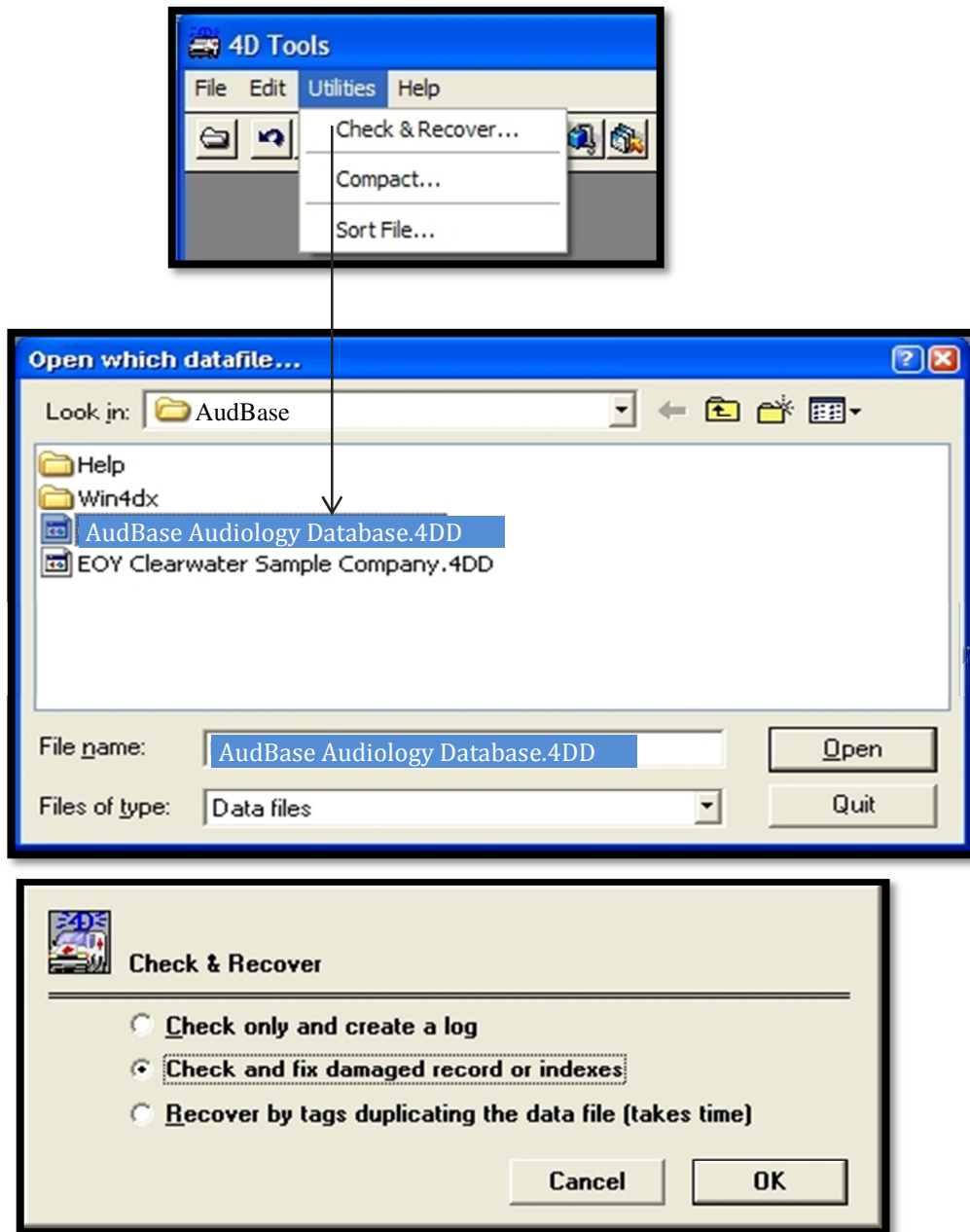
AudSoft will perform database maintenance once a year to ensure that your data file is kept to the minimum possible size for backups and to maintain file efficiency and integrity. The database maintenance routine will be performed annually in accordance with the support contract or on a frequency as specified by the customer and agreed to in contract.

### Tools Available For Maintenance



Compact - This tool compacts the database to its minimum possible size and ensures minimum latencies when addressing the database or when rendering data for queries.

## Tools Available for Repair and Recovery



Check only and create a log - This tool identifies database errors and provides a log of found or known errors.

Check and fix damaged indexes - This tool identifies database errors and corrects them.

Recover by tags - This tool will create a totally new data file, while incorporating the repaired contents of the original data file.

Restore - This utility allows you to restore the database to an earlier predefined point in time. This works the same as a Windows System Restore.

## Server Vulnerability - Catastrophic Failure

Another point of potential vulnerability is hardware failure. In the event of hardware failure there are options to limit or nullify downtime. These options are dependent on whether the server is operating in a virtual or physical environment.

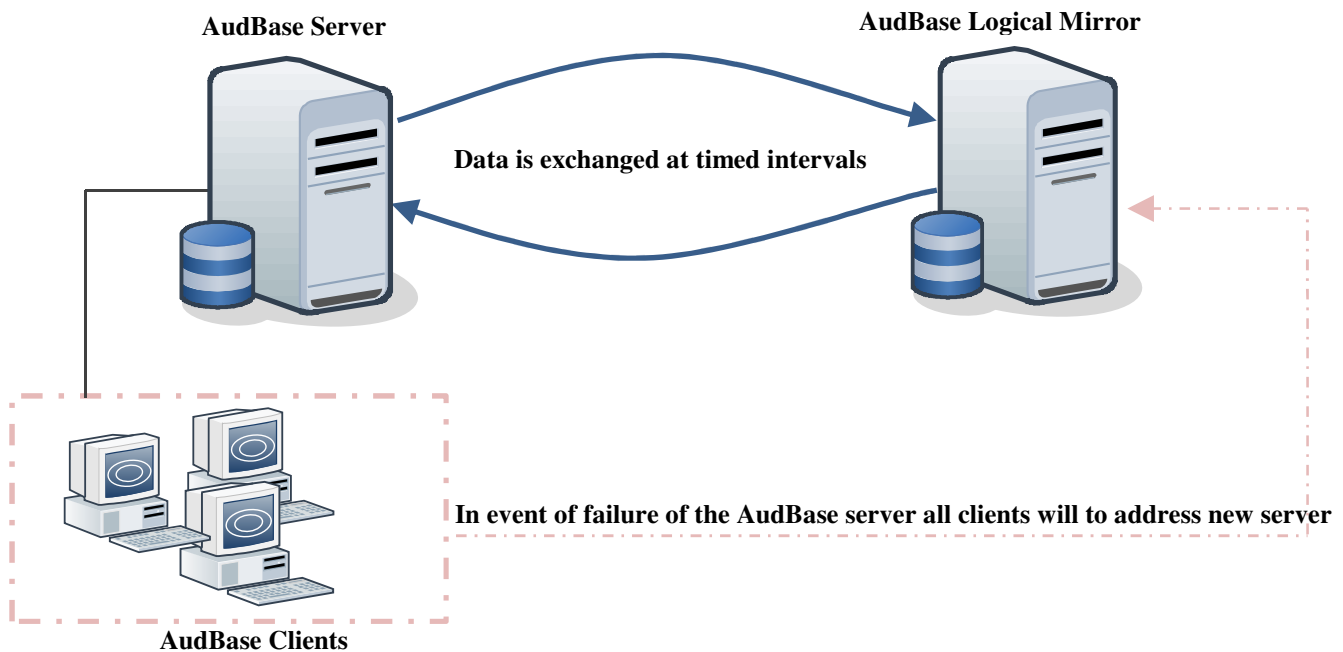
One option that can be employed, if the server is running in a virtual environment, is to replicate the old server using an image creation process. Reimage a new server using old server image from backup files.

If running server in a physical environment, you would have to employ a “mirrored server” or “logical mirror” strategy. A logical mirror is a sophisticated backup mode, primarily intended for critical or high-load databases.

Using a logical mirror consists in operating a database on one machine and keeping a copy of it that is periodically updated on a second machine. Both machines communicate via the network with the machine in operation regularly transmitting any changes made in the database to the mirror machine via the intermediary of the log file.

In this way, when there is an incident affecting the operational database, the mirror database can be used to get things back in working order quickly without any data loss. Moreover, the operational database is never “blocked” by backup operations.

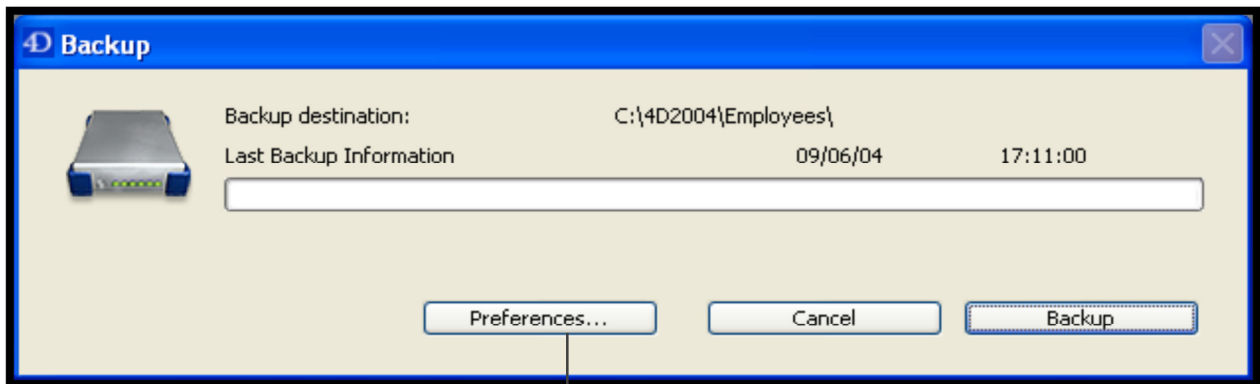
Upon hardware failure the only two actions required is for the startup of the AudBase service on the server, and for the end user to key into the client the associated IP of the new (mirrored) server.



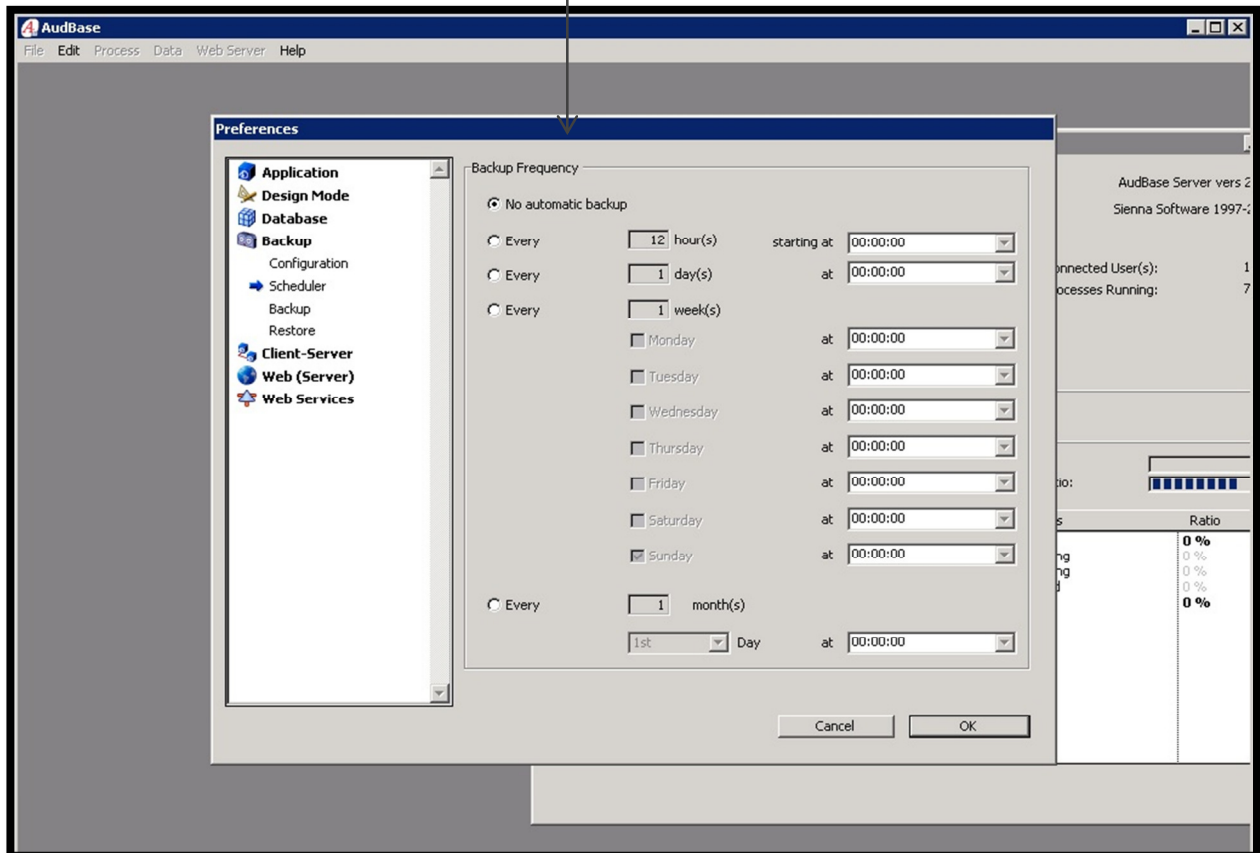
### Server / Database Backup

The server control panel on the AudBase Server includes a complete database backup and restore utility module. This module allows the backup of the database during operation, without having to exit the application. Backups can be launched manually or automatically, at regular intervals, and without user intervention. In the event of an incident, restoring and/or restarting the database can also be initiated automatically.

Backups can run automatically through the backup scheduler or manually. Using the scheduler, backups can be set for random times or defined intervals. Backup should consist of Flat file backup of c:\program files (x86)\audbase\. This can be done while the system is running without having all clients log off.



### Backup Scheduler Utility:



### Security Feature Chart

ITEM	AudBase
Password Attempts/Logons recorded to Log file	●
All Actions within Application recorded to Log file	●
All interface transactions recorded to Log file	●
Log file archiving	●
Idle "time out" function--- <i>automatic timed Log Off</i>	●
Extensive Customizable Password Criteria	●
Extensive Granular User Access Controls (UAC)	●
Anonymity Viewing feature for User Access Control	●
Record Locking System for Non Admin. Users	●
Encryption between Client and Server	●
Virtual Environment Compatible	●
Checksum Process--- <i>verifies integrity of data in database</i>	●
Complete Backup Scheduler and Utility	●

### Example Log Files

#### Password Login

Date	Date format	Time	Login Name
1/5/2015	1	22:51:02	administrator
1/6/2015	1	18:49:45	administrator
1/7/2015	1	13:40:55	administrator
1/7/2015	1	13:40:55	administrator
1/7/2015	1	20:39:14	administrator
1/7/2015	1	20:39:19	administrator
1/19/2015	1	14:26:50	administrator
1/19/2015	1	15:10:33	manny
1/19/2015	1	15:11:52	manny
1/19/2015	1	15:11:53	manny
1/19/2015	1	15:14:44	administrator
1/19/2015	1	15:14:52	administrator

#### Record Modifications / Actions

Table/ID Field Key:							
Table#	Table name	ID Field#’s	Access				
5	[Provider]	# 1	V-(View)				
6	[ClinicalGroup]	# 1	W-(Write)				
8	[Subject]	# 1					
12	[Audiogram]	# 1, # 5					
13	RT_WordRecog	# 1, # 5					
14	Tympanogram	# 1, # 5					
Date	Date format	Time	User ID	Access Type	Table#	ID Field Value(s)	Modified field#s
11/6/2014	1	13:04	43000	W	5	46000;	
11/12/2014	1	17:11	-2	W	12	687000, 451000	[Auto-save or other function may have masked modified field info];
11/12/2014	1	18:03	-2	W	14	687000, 451000	[Auto-save or other function may have masked modified field info];
11/12/2014	1	18:03	-2	W	13	687000, 61000	[Auto-save or other function may have masked modified field info];
11/12/2014	1	18:03	-2	W	12	687000, 451000	[Auto-save or other function may have masked modified field info];
11/17/2014	1	19:14	-2	W	8	90000;	
11/17/2014	1	19:21	-2	W	8	111000;	
11/17/2014	1	19:32	-2	W	8	177000;	
11/17/2014	1	19:44	-2	W	8	215000;	
11/17/2014	1	20:42	-2	W	8	724000;	
11/17/2014	1	20:46	-2	W	8	1000;	
11/17/2014	1	20:47	-2	W	8	2000;	
11/21/2014	1	11:27	-2	W	8	136000;	
11/21/2014	1	11:30	-2	W	8	136000;	
11/27/2014	1	21:38	-2	W	12	136000, 346000	[Auto-save or other function may have masked modified field info];
12/8/2014	1	11:39	-2	W	13	721000, 63000	9, 10, 12, 39, [Auto-save or other function may have masked modified field info];
12/8/2014	1	11:39	-2	W	12	721000, 460000	11, 13, 14, 15, 17, 22, 481, 495, [Auto-save or other function may have masked modified field info];
12/8/2014	1	11:40	-2	V	12	721000, 460000;	
12/8/2014	1	11:40	-2	V	13	721000, 63000;	