

Configuring and Managing Your



PROFESSIONAL

Version 8.0



Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictional unless otherwise noted. No portion of this document or the accompanying software may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopy, recording or otherwise, for any purpose, without the express written permission of Second Opinion Telemedicine Solutions, Inc.

Copyright © 1998-2012 by Second Opinion Telemedicine Solutions, Inc. All rights reserved.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Every effort has been made to ensure complete and accurate information concerning the material presented in this document. However, Second Opinion Telemedicine Solutions, Inc. can neither guarantee nor be held legally responsible for any mistakes in printing or faulty instructions contained in this document. The author always appreciates receiving notice of any errors or misprints.

Please remember: You must accept the enclosed License Agreement before you can use this product. The product is licensed as a single product. Its component parts may not be separated for use on more than one computer. If you do not accept the terms of the License Agreement, you should promptly return the product for a refund. Do not make illegal copies. For further details, please refer to the License Agreement.

Contents

The Professional Administrator...5

- What it Does...5
- Second Opinion Security Model...5
 - Rights*
 - User Groups*
 - Strategies for Creating User Accounts*
- How Second Opinion Tracks Information...8
 - Station*
 - Site*
 - The Shared Database*
- Available Rights...9
 - Access to Folders*
 - Access to Documents and Forms*
 - Other Rights*
 - Administrator Right*
- Predefined Sample User Groups and Accounts...12
- Start the Professional Administrator...14
- Define User Groups...15
 - Create a new group*
 - Modify a group's properties*
 - Delete a group*
- Define User Accounts...17
 - Create a new user*
 - Modify a user's properties*
 - Delete a user*
- Define Site Information...19
 - Create a New Site*
 - Modify a Site's Properties*
 - Delete a Site*
- Perform Database Maintenance...21
 - Manage or Clean Up a Specific Table*
 - Clean Up All Tables*
- Maintain System Files...22
 - Manage System Access Tables*
 - Delete or Rename Tables and Fields*
 - Insert New Table into System Access Database*
- Audit Log...24
 - Set Audit Tracking Level*
 - View Audit Log Entries*
- Enter Authorization Codes...25
 - If You are Registering for the First Time*

Contents

Index...26



The Professional Administrator

What it Does

Second Opinion Professional is designed to be used in a wide variety of environments; from a single computer being used by a single user to multiple computers connected across a local or wide area network, accessed by multiple, possibly roaming, users.

The Administrator program allows you to define users and their security rights, as well as define and maintain other system functions.

Second Opinion Security Model

Second Opinion Professional has been designed to control access to sensitive information. Its security model allows you to define what information each user can see and what actions they can perform. This is done in two steps: 1) create user groups, and 2) create user accounts. Before you begin to create user accounts, take some time to organize how you wish to group your users, what access each group of users will have, and how you will define user Login Names and Password controls. While it is relatively easy to change user and group information at any time for a small set of users (half a dozen or less), it can become confusing when the user base grows to several dozen or more, spread out across several sites. Taking time to organize this now will save you headaches later on when you have to explain why a user can not do *this* or have access to *that*.

Rights

A right is an ability to perform an action. If a user is assigned a right, then the user can perform the actions that require that right. Examples of rights include: the ability to create, view, edit, and/or delete records.

For a detailed description of the available rights, see “Available Rights,” page 9.

User Groups

A group is a collection of one or more rights. This makes it easy to manage a set of users with similar requirements without having to go to each user's properties to add or remove rights. Examples of user groups include: system administrators, users that can create records, and users that can only view records.

Second Opinion Professional ships with a number of pre-defined user groups and user accounts that are designed with typical needs in mind. If these pre-defined groups do not meet your needs, you should modify them or create your own. For a detailed description of the pre-defined user groups, see "Predefined Sample User Groups and Accounts," page 12.

You can assign a user to multiple groups, thereby creating various combinations. For example, the pre-defined user account "SOUSER" belongs to the groups "GLOBAL USERS," "ARCHIVE OPERATORS," and "CONFERENCE PARTICIPANTS," allowing that user to participate in all those activities.

When you create a user group, give that group only the minimum rights necessary for all of the users that will belong to that group to perform the tasks they need to perform. If you have a subset of those users that need additional rights, either create a separate group with those additional rights and assign those users additional membership to that group (as in the pre-defined account "SOUSER"), or create an entirely separate group with all of the rights for those users (as in the pre-defined account "SOGUEST").

Strategies for Creating User Accounts

When you create user accounts in Second Opinion, you should consider the following:

Logon Names

- If your users already have individual Windows or network logons, use that same name for the Logon Name in Second Opinion. This way your users only have to remember one name.
- If your users do not already have Windows or network logons or use a common/shared Windows logon, create a unique Logon Name for Second Opinion. Good name creation strategies include: 1) part names (e.g., BILLG, TIMR, ROBF), 2) full names (e.g., BILLGREEN, TIMRUSSEL, ROBF FRANCIS), and 3) user initials and an incremental number to deal with duplicate names (e.g., AJM39, DTR20). The method you use is entirely up to you; but it should be consistent.

Passwords

- Without exception, every user account on a network should have a password, even though Second Opinion allows you to forgo this security. Passwords exist to make both the user account and the program's information inaccessible to prying eyes.
- The ideal password is memorable, yet uncrackable. If you wish to allow your users to be able to change their own passwords, give the security group they belong to the "Change password" right. To prevent them from changing it to an empty one, also assign the "Requires password" right. A good password is made up of a combination of characters and numbers and is at least six characters long. Do not use the Logon Name as the password.
- You should always change passwords in these circumstances: when a user leaves (if you leave the user account open), when a system administrator leaves, any time you suspect an intrusion has occurred through an account (Second Opinion can log all user access attempts), where any user has allowed his or her password to be known by others, and regularly for administrative accounts as a precaution. As a general rule, the more power an account has over the system, the more often the password should be changed.

How Second Opinion Tracks Information

When you install Second Opinion Professional, especially across a network, it is important to understand how the program tracks information. This is to ensure that all security settings and access capabilities are set up appropriately for your environment.

Security rights are available to allow you to control what information users can see.

Station

A station (sometimes called a workstation) is an individual computer running Second Opinion. Your license defines the maximum number of stations that can run the program and share the same database at the same time. If one more station tries to run the program than has been authorized by the license, the user will get a warning message and the program will not start.

Site

A site represents a specific physical location (such as a building or portion of a building) or logical grouping (such as a division) with one or more stations using a single, shared Second Opinion database.

Each site is assigned a different Site Code. You can contact Second Opinion Telemedicine Solutions, Inc. to obtain additional Site Codes.

Each user defined to use the system must be associated with a specific site. When a record is created it is associated with both the physical site and the user's site. This allows a user to go to a station at a different site on the shared database to view their data.

The Shared Database

Each installation of the Second Opinion database is assigned a unique Database ID. One or more stations can share/use the database at the same time (up to the license limit) over a local area network (LAN), or wide area network (WAN) .

Since information in Second Opinion can be sent to and received from computers not connected/sharing your database, the system uses the Database ID to determine who owns what records. You are not allowed to edit in any way information that was created on a different database and imported into your database.

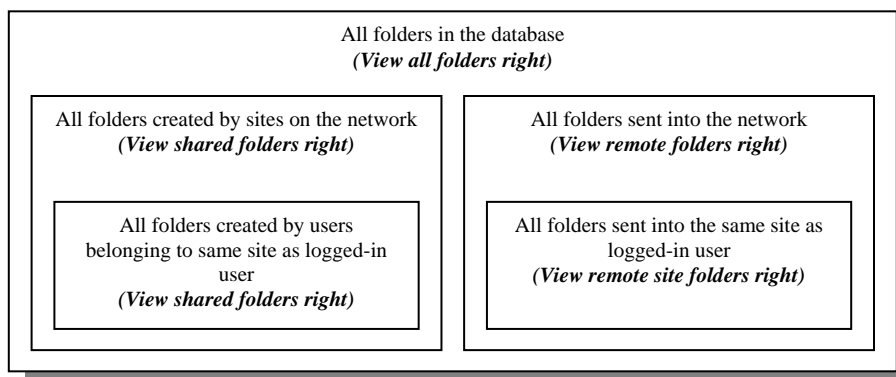
Available Rights

Access to Folders

Users can only see folders at the level they have the right to.

Right	If user has this right, user can:
View site folders	See only folders created by other users that also belong to the same site. This is the most restrictive level.
View remote site folders	See only folders sent directly to this site from outside the network. Folders are sent in using communications, electronic mail, or imported (usually through Second Opinion Data files). A user cannot see records sent to other sites on this network.
View shared folders	See all folders created by any site sharing the same database. A user cannot see records that were created outside of the database and were sent in using communications, electronic mail, or were imported. Implies “View site folders” right.
View remote folders	See all folders sent to any site on this network from outside the network. Folders are sent in using communications, electronic mail, or imported. Implies “View remote site folders” right.
View all folders	See all folders in the system, regardless of who created them. This is a combination of “View shared folders” and “View remote folders.”

If a user has none of the above rights, then the user cannot see any folder information. The following diagram illustrates the scope of the various view folder rights:



Users that are creating, editing or deleting folders also need one or more of the following rights.

You also need one of the View folder rights to access the folder record.

Right	If user has this right, user can:
Create folders	Create new folders associated with this site. Implies “View site folders,” “Create documents,” and “View documents” rights.
Edit folders	Edit information of existing folders. Implies “view site folders” right.
Export folders	Export, send, or copy existing folder information for transfer outside the system using communications, electronic mail or export features.
Delete folders	Delete existing folders.

Access to Documents and Forms

Right	If user has this right, user can:
View documents	View existing documents.
Create documents	Create new documents or forms. Implies “View documents” right.
Edit site documents	Edit information for existing documents or forms that were originally created by a user belonging to the same site. Implies “View documents” right.
Edit shared documents	Edit information for documents or forms created by any site sharing the same database. Implies “Edit site documents” and “View documents” rights. A user cannot edit records that were created outside of the network and sent in using communications, electronic mail, or were imported.
Export documents	Export, send, or copy documents for transfer outside the system.
Annotate	Annotate documents in the Image Viewer.
Delete documents	Delete documents or forms.

You need the View documents right to access documents.

Other Rights

Right	If user has this right, user can:
Archive	Use the Archive program to archive or restore information.
Edit preferences	Change non-security related system preferences such as colors, etc.
Change password	Change his/her own login password.
Requires password	User requires password to log in. A user cannot change his/her password to a blank one.

Administrator Right

The “Administrator” right is a special right that automatically gives a user all of the above rights and full access to the system. It is required for using the Professional Administrator program.

Be careful who you give the “Administrator” right to.

Predefined Sample User Groups and Accounts

The program ships with the following predefined user groups and accounts.

Sample User Groups

Group	Members of this group:	Rights
ADMINISTRATORS	Have all rights.	Administrator
SITE USERS	Have access to only folders created by this site. Cannot access folders created by other sites.	Annotate Create documents Create folders Edit site documents Edit folders Export documents Export folders Change password Requires password View documents View site folders
SITE VIEWERS	Have view-only access to only folders created by this site.	View documents View site folders
SHARED USERS	Have access to all folders created by sites using the shared database. Cannot access folders created by other networks.	Annotate Create documents Create folders Edit site documents Edit site folders Export documents Export folders Change password Requires password View documents View shared folders
SHARED VIEWERS	Have view-only access to all folders created by any site sharing the same database. Cannot access folders created by other networks.	View documents View shared folders

GLOBAL USERS	Have access to all folders.	Annotate Create documents Create folders Edit shared documents Edit folders Export documents Export folders Change password Requires password View documents View all folders
GLOBAL VIEWERS	Have view-only access to all folders.	View documents View all folders
CONFERENCE PARTICIPANTS	Have access to folders sent to the network by other sites.	View remote folders
ARCHIVE OPERATORS	Can archive information.	Archive

Sample users

Login Name	Password	Belongs to Groups	Description
SOSAMPLE	1234	ADMINISTRATORS	Has full access to the system. Use this login to enter the Administrator program until you create another user with the "Administrator" right.
SOUSER	1234	GLOBAL USERS, ARCHIVE OPERATORS, CONFERENCE PARTICIPANTS	Has typical user access. User can create, edit, and view information.
SOGUEST	(None)	GLOBAL VIEWERS	Has typical view-only access.



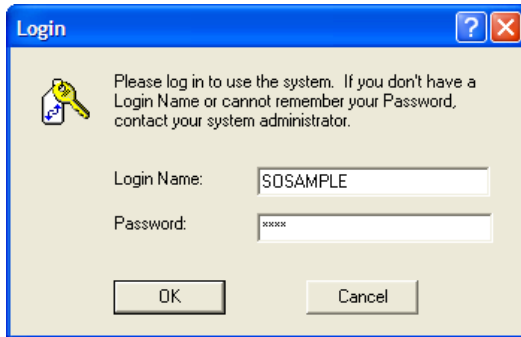
NOTE: After you have become familiar with Second Opinion and its various components and are ready to begin using the system with real data, you should create real users and remove the sample users. If you do not do this, it will be easy for an unauthorized user to gain complete access since all copies of Second Opinion ship with these samples.

Start the Professional Administrator

1. Click **Start, Programs, Second Opinion, Professional Administrator**.
2. When the program starts, a dialog box will prompt you to log in.



Professional Administrator application icon



3. You must enter a valid **Login Name** and **Password** before you can access any of the functionality of the program. You must also have the Administrator right. Click **OK** when you have entered the information.
4. The main program window now appears.

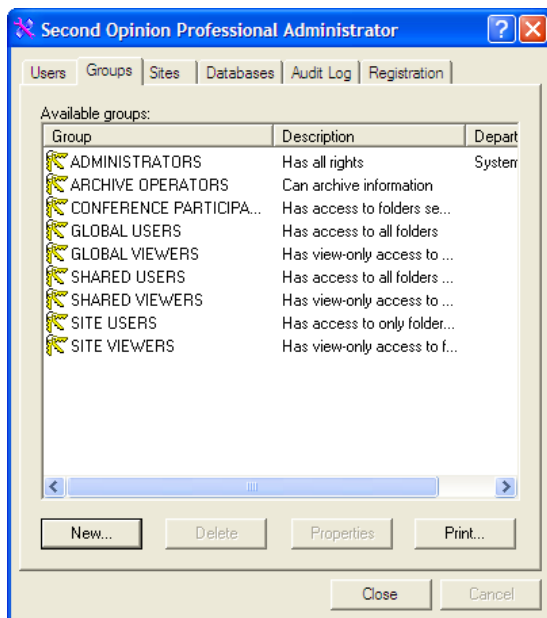
If this is the first time you are using the program, log in as "SOSAMPLE" with "1234" as your password.



NOTE: If you cannot remember the login name or password, you must contact Second Opinion Telemedicine Solutions, Inc. Customer Support. We will require appropriate identification to restore your access.

Define User Groups

To define user groups, select the **Groups** tab in the main window.



Create a new group

1. Click **New**.
2. Enter a name and description for the group. Enter the department name if the group will be used by a particular department.
4. Click **Next** and add any existing users you want to belong to this group (to define users, see “Define User Accounts,” page 17).
5. Click **Next** and add the rights you wish members of this group to have (for a description of the available rights, see “Available Rights,” page 9).
6. Click **Finish** to add the group.

Modify a group's properties

1. Select the group you wish to modify.
2. Click **Properties**.
3. Alter any information on any page.
4. Click **OK** to apply the changes.

Delete a group

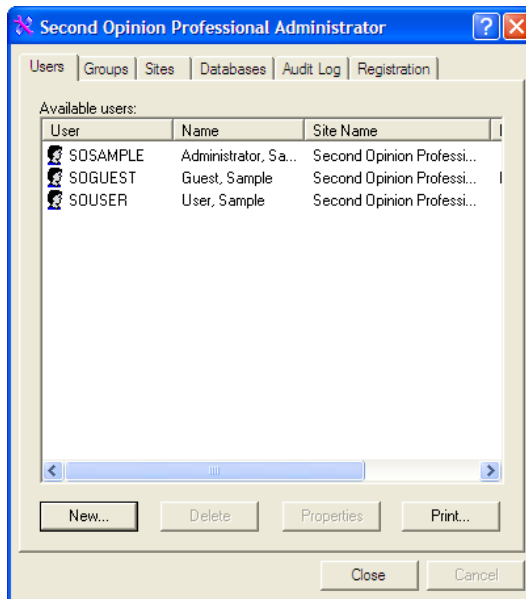
1. Select the group you wish to delete.
2. Click **Delete**. The program will ask you to confirm; click **Yes**.



NOTE: The Professional Administrator program requires that at least one group contains the “Administrator” right and that at least one user belongs to it. If you somehow exit the program with no user possessing the “Administrator” right, you must contact Second Opinion Telemedicine Solutions , Inc. Customer Support. We will require appropriate identification to restore your access.

Define User Accounts

To define users, select the **Users** tab in the main window.



Create a new user

1. Click **New**.
2. Enter the desired **Login Name** for the user. No other user in the system should have this login name. Also enter the user's first, middle and last name.
3. Enter any other available identification information about the user.
4. Click **Next** and choose the site the user is to be associated with.
5. Click **Next**. If the user has phone numbers that are different than the site's, fill them in.
6. Click **Next**. Enter a **Password** for this user and again in the **Confirm Password** field.
7. Click **Next** and add any groups you want the user to belong to (to define groups, see "Define User Groups," page 15).
8. Click **Finish** to add the user.



NOTE: The current version of Second Opinion does not use the **Account has expiration date** and **Force periodic password change** features.

Modify a user's properties

1. Select the user whose configuration you wish to modify.
2. Click **Properties**.

3. Alter any information on any page.
4. Click **OK** to apply the changes.

Delete a user

1. Select the user you wish to delete.
2. Click **Delete**. The program will ask you to confirm; click **Yes**.



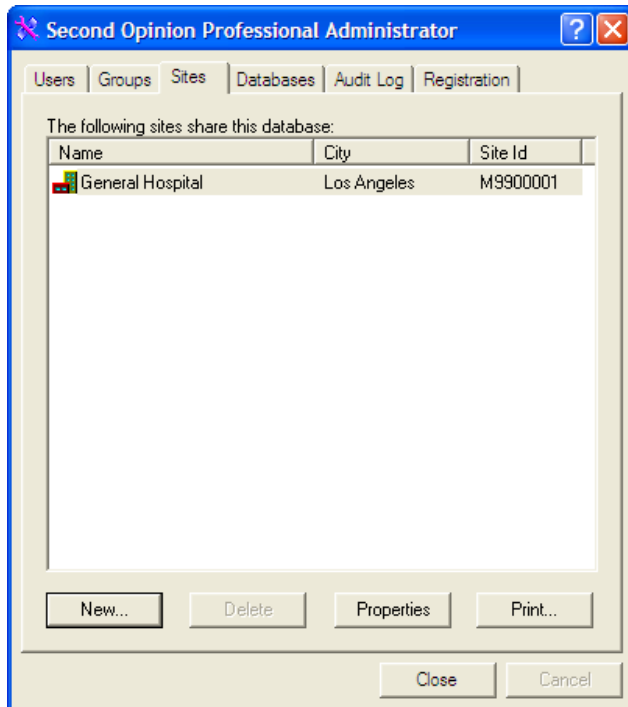
NOTE: The Professional Administrator program requires that at least one user belongs to a group with the “Administrator” right so that the user can log back into the program. If you somehow exit the program with no user possessing the “Administrator” right, you must contact Second Opinion Telemedicine Solutions, Inc. Customer Support. We will require appropriate identification to restore your access.

Define Site Information

For information on what sites are and how they are used, read “How Second Opinion Tracks Information” on page 8.

Second Opinion requires that you enter information about each individual site. You can only define as many sites as you have Site Codes.

To enter site information, select the **Sites** tab in the main window.



Create a New Site

Before creating a site, you must have a Site Code assigned by Second Opinion Telemedicine Solutions, Inc.

1. Click **New**.
2. Enter the **Site Code** assigned to you.
3. Click **Next** and enter the site name, and other optional information.
4. Click **Next** and enter the site's address.
5. Click **Next** and enter the site's central voice and fax numbers.
6. Click **Finish** to add the site.

Modify a Site's Properties

1. Select the site you wish to modify.
2. Click **Properties**.

3. Alter any information on any page.
4. Click **OK** to apply the changes.

Delete a Site

1. Select the site you wish to delete.
2. Click **Delete**. The program will ask you to confirm; click **Yes**.



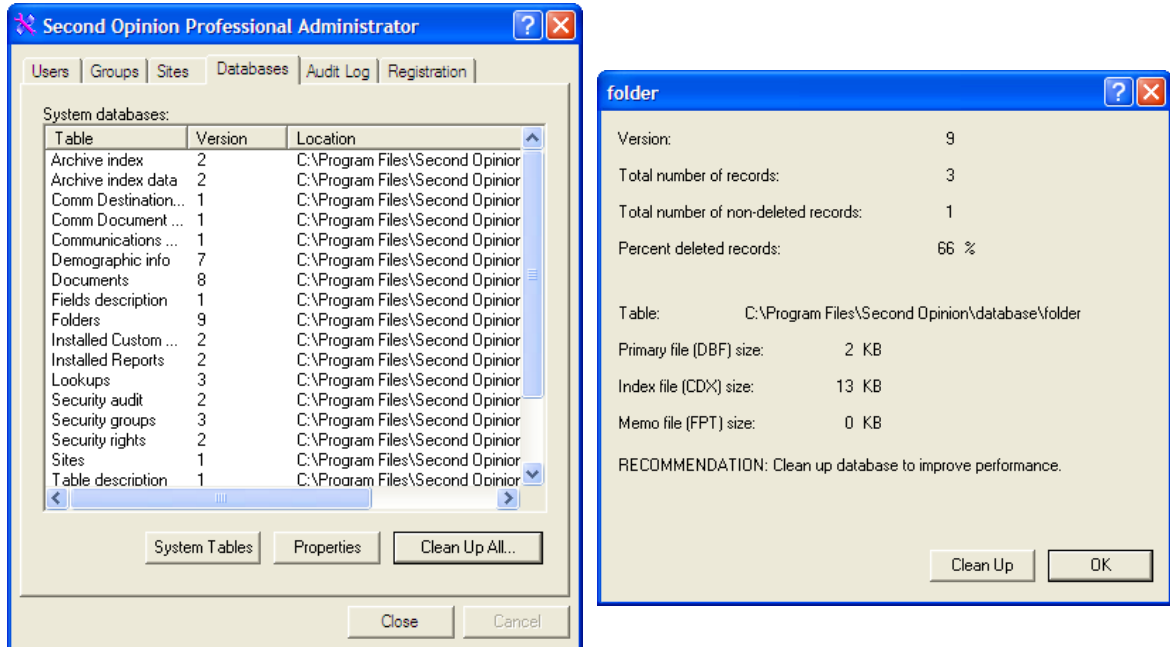
NOTE: You should always have at least one site defined so that Second Opinion has information about where it's installed.

Perform Database Maintenance

You should periodically clean up the Second Opinion database tables to ensure any deleted records are purged from the system. This will reduce the size of the database and improve performance.

Before you do this, make sure no other user is using Second Opinion anywhere on the system.

To perform database maintenance, select the **Databases** tab from the main window.



Manage or Clean Up a Specific Table

1. Select the desired table.
2. Click **Properties**.
3. To clean up a table, click **Clean Up**. When asked if you wish to re-create the index files to fix possible database corruption problems, click **Yes**. Second Opinion will open each table and clean it up. If it finds any problems, it will inform you and attempt to fix them. If any problems are found, we recommend that you repeat the procedure to ensure no further problems are identified.

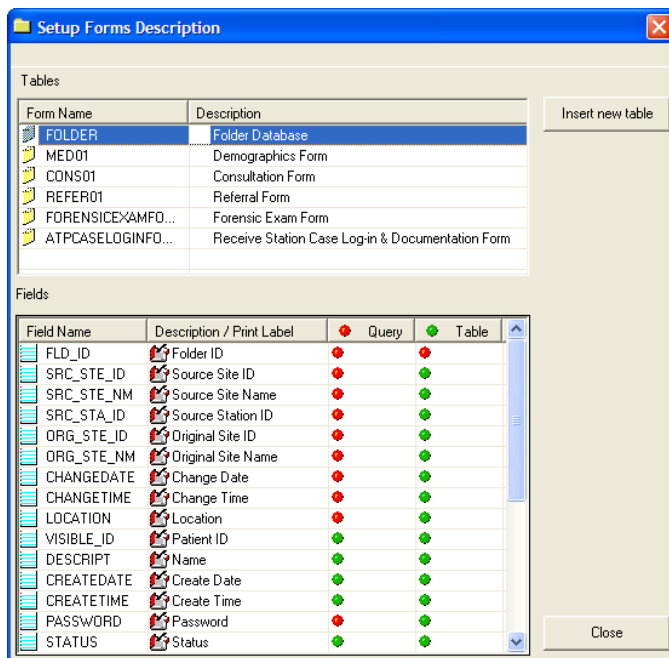
Clean Up All Tables

To process all of the database tables in the list, click **Clean Up All**.

Maintain System Files

WordReport and the Advanced Search Engine have the ability to access all of the databases within Second Opinion. Some of these databases contain system information that is not useful data from an end user standpoint. Other databases contain information that is private and should remain confidential and not used for reporting or searching purposes. The System Files Maintenance function gives the System Administrator the ability to restrict what users have access to when creating reports and performing advanced searches.

To perform this operation, select the **Databases** tab from the main window.



Manage System Access Tables

1. Click **System Tables**.
2. Select the desired table, then for each field within the table click whether or not it should be available for reporting (Table) or search functions (Query).

Green indicates the field is available

Clicking on the **Query** or **Table** column header changes all of the values within the column.

Delete or Rename Tables and Fields

Right Click the desired Table or Field and select **Delete** or **Rename**.

Insert New Table into System Access Database

Click the **Insert new table** button.

The screenshot shows the 'Setup Forms Description' dialog box. It has two main sections: 'Tables' and 'Fields'. The 'Tables' section contains a table with two columns: 'Form Name' and 'Description'. The 'Fields' section contains a table with four columns: 'Field Name', 'Description / Print Label', 'Query', and 'Table'. On the right side of the dialog, there are buttons for 'Show All Forms', 'Show All Tables', 'Browse', 'Insert', 'Cancel', and 'Close'.

Show All Forms will display all of the Second Opinion Custom Forms that have been registered within the system.

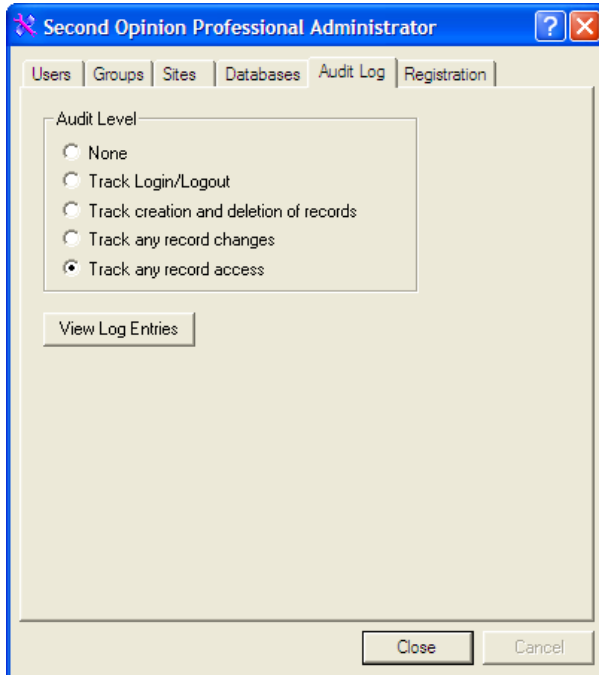
Show All Tables will display all of the database contained in the Second Opinion database directory.

Browse enables you to browse using an explorer window to select a desired database table.

The screenshot shows the 'Setup Forms Description' dialog box after the 'Show All Tables' button was clicked. The 'Tables' section now contains one entry: 'ForensicExamForm20...' with description 'Forensic Exam Form'. The 'Fields' section is populated with a list of fields including TEMPLATEID, FLD_ID, DOC_ID, CHANGEDATE, CHANGETIME, FVISIBLEID, FDESCRIPT, CASENUM, ARDATE, ARTIME, EXAMINER, LEONAME, LEODID, LEODEPT, and PADVOCATE. The 'Show All Forms' button is highlighted.

Audit Log

Second Opinion can track which users are using the program and what activities are performed.



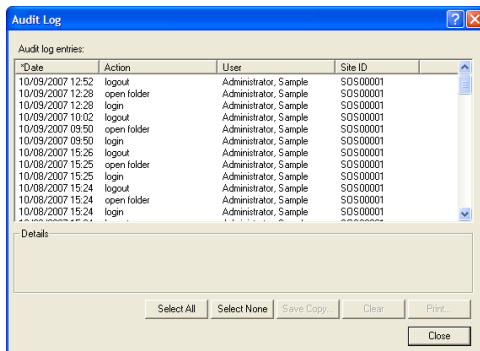
Set Audit Tracking Level

You can track which users are using Second Opinion and what activities they are performing by setting the Audit Level to one of four levels:

1. Select the **Audit Log** tab from the main window.
2. Choose the desired **Audit Level**.

View Audit Log Entries

To view the audit log, click on the **View Log Entries** buttons.

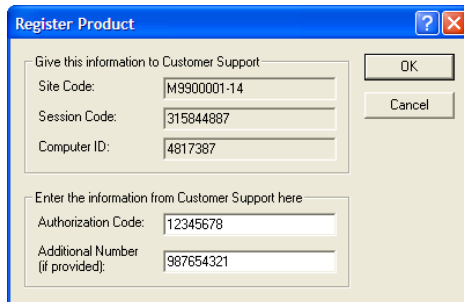


Enter Authorization Codes

Authorization Codes are used to unlock specific application functionality, including converting a demonstration copy to a full copy, increasing local area network (LAN) licensed simultaneous users, and extending or removing limits.

If you need to enter an Authorization Code:

1. Choose the **Registration** tab from the main window.
2. Click **Register Application**.



The screenshot shows a dialog box titled "Register Product" with a blue title bar and standard window controls. It is divided into two sections. The top section, "Give this information to Customer Support", contains three text input fields: "Site Code" with the value "M9900001-14", "Session Code" with "315844887", and "Computer ID" with "4817387". To the right of these fields are "OK" and "Cancel" buttons. The bottom section, "Enter the information from Customer Support here", contains two text input fields: "Authorization Code" with "12345678" and "Additional Number (if provided)" with "987654321".

If You are Registering for the First Time

1. Copy the **Site Code**, **Session Code**, and **Computer ID** to the Registration Form.PDF file included on your CD.
2. Complete and either email or fax the Registration Form to Second Opinion Telemedicine Solutions, Inc.
3. When Second Opinion Telemedicine Solutions, Inc. issues you an Authorization Code and Additional Number, enter them in the Register Product window and click **OK**.

A

Access, controlling, 7
 Administrator
 defined, 7
 logging in, 16
 starting, 16
 Administrator program, 7
 Administrator right, 13
 Annotate right, 12
 Archive right, 13
 Audit Log
 tracking level, 26
 viewing, 26
 Authorization Code, 27

C

Change password right, 13
 Create documents right, 12
 Create folders right, 12
 Creating new
 sites, 21
 user groups, 17
 users, 19

D

Database ID, defined, 10
 Database, maintenance, 23
 Databases, sharing, 10
 Delete documents right, 12
 Delete folders right, 12
 Deleting
 sites, 22
 user groups, 18
 users, 20
 Documents, rights to access, 12

E

Edit folders right, 12
 Edit preferences right, 13
 Edit shared documents right, 12
 Edit site documents right, 12
 Export documents right, 12
 Export folders right, 12

F

Folders, rights to access, 11

G

Groups. *See* User groups

L

LAN, 10
 Local Area Network, 10
 Logging in, 16
 Login Names
 Windows logon, 9
 Login Names, defining, 19
 Logon Names
 creating, 9

M

Modifying
 sites, 21
 user groups, 17
 users, 19

P

Passwords
 changing, 9
 creating, 9
 Passwords, defining, 19

R

Registering, 27
 Requires password right, 13
 Rights
 defined, 7
 how to use, 11
 list of, 11

S

Security
 Administrator program, 7
 Audit Log. *See* Audit Log
 model, 7
 tracking information, 10
 user groups, defined, 8
 Site Code, 10
 Sites
 creating new, 21
 defined, 10
 deleting, 22
 modifying, 21

- property pages, 21
- Stations, defined, 10
- System File, maintenance, 24

U

- User groups
 - creating new, 17
 - defined, 8
 - deleting, 18
 - list of available rights, 11
 - modifying, 17
 - predefined, 14
 - property pages, 17
- Users
 - Administrator right requirement, 20
 - creating new, 19
 - creation strategies, 9
 - delete, 20

- Login Name, 16, 19
- modify, 19
- Password, 16, 19
- predefined, 15
- property pages, 19

V

- View all folders right, 11
- View documents right, 12
- View remote folders right, 11
- View remote site folders right, 11
- View shared folders right, 11
- View site folders right, 11

W

- WAN, 10