# Table of Contents

1. *Getting Started* .............................................................................................................. 1
   1.1 System Requirements ............................................................................................... 1
       1.1.1 Workstations ....................................................................................................... 1
       1.1.2 File server/networks ............................................................................................ 3
       1.1.3 Windows networking (“Peer-to-Peer”) ............................................................... 3

2. *Overview* ........................................................................................................................ 4
   2.1 What’s New in the Data Store Administration Tool 2014? ........................................ 5
   2.2 Installing the Data Store Administration Tool ............................................................ 6
   2.3 Data Store Best Practices ......................................................................................... 7

3. *Creation and Connection* ............................................................................................. 8
   3.1 Creating a Data Store ................................................................................................ 8
       3.1.1 Setting up an xBase Data Store ......................................................................... 9
       3.1.2 Setting up a SQL Server Database: .................................................................... 10
   3.2 Connecting to a Data Store ..................................................................................... 15
       3.2.1 To connect to an existing Data Store using the program: ................................. 15
       3.2.2 To connect to an existing Data Store using the Connection (.cwc) file: .......... 16
       3.2.3 To disconnect from a Data Store using a Disconnection (.cwc) file: .............. 16
   3.3 Turning off Auto Close in the SQL Server ............................................................... 16
   3.4 Creating Connection (.cwc) Files ............................................................................ 16
   3.5 Create/Connect tab ................................................................................................. 17
   3.6 Viewing the status of the Data Store ....................................................................... 18

4. *Managing Users* .......................................................................................................... 19
   4.1 Populating the User List .......................................................................................... 19
   4.2 Connect to Active Directory Server dialog ............................................................... 19
   4.3 Importing/Adding users from the Active Directory ................................................... 19
   4.4 Adding users from the Windows Active Directory ................................................... 20
   4.5 Active Directory Import ............................................................................................ 20
   4.6 Active Directory tab ................................................................................................. 23
   4.7 Enabling Windows Active Directory ......................................................................... 24
   4.8 Active Directory Integration dialog ........................................................................... 24
   4.9 Adding a Login Using SQL Server Management Studio ......................................... 26
   4.10 Using LDAP Import Filters ..................................................................................... 27
   4.11 Using Command Prompt for Import Filter ............................................................. 28

5. *Settings* ........................................................................................................................ 30
Chapter 5: Accounting and Financial Records

5.1 Security ID overview ................................................................................................ 33
5.2 Setting the Security ID ............................................................................................. 35
5.3 Disabling the Security ID ......................................................................................... 35

6. Maintenance ................................................................................................................ 36

6.1 Maintenance | Import option .................................................................................... 37
6.2 Export or Import Users and Groups dialog .............................................................. 37
6.3 Working Papers Databases ..................................................................................... 38
6.4 Database files .......................................................................................................... 38

7. Advanced Options and Troubleshooting ................................................................. 39

7.1 Overview .................................................................................................................. 39
7.2 Software Environment ............................................................................................. 40
7.3 Lifecycle ................................................................................................................... 40
7.4 Registry ................................................................................................................... 41
7.5 Folder Security ........................................................................................................ 42
7.6 Backing Up .............................................................................................................. 42
7.7 Maintenance ............................................................................................................ 43
7.8 Making the Data Store Read-Only .......................................................................... 45
7.9 File Tracking ............................................................................................................ 46
7.10 Troubleshooting ..................................................................................................... 48

8. Upgrading from previous versions of Working Papers .......................................... 49

9. Getting Technical Support ......................................................................................... 50
1. Getting Started

1.1 System Requirements
CaseWare® Working Papers requires minimum machine and software requirements for:

- **Workstations**
- **File server/networks**
- **Windows networking ("Peer-to-Peer")**

1.1.1 Workstations

**Operating systems**

- Microsoft Windows 8 or higher
- Microsoft Windows 7 Professional Service Pack 1 or higher
  
  **Note:** See [here](#) for important information when sharing files hosted on Windows 7.
- Microsoft Windows Vista Service Pack 2 or higher
  
  **Note:** See [here](#) for important information when sharing files hosted on Windows Vista.
- Microsoft Windows XP Professional Service Pack 3 or higher*

*On April 8, 2014, Microsoft will end their support for Windows XP and Office 2003. On that date, Windows XP and Office 2003 will no longer be supported for any CaseWare products. Please visit [http://www.caseware.com/support](http://www.caseware.com/support) to view a list of supported Windows operating systems for our products.

**Hardware**

- 1 GHz 32-bit (x86) or 64-bit (x64) processor
- Minimum 512 MB of system memory; 1,024MB or more recommended for improved performance.
- The Working Papers program requires 150 MB hard drive space.
- The size of open client files will vary depending on the features used and the size of documents managed. Working Papers has built-in compression that significantly reduces the size of compressed files.
- SVGA monitor capable of 256 colors and 800x600 resolution is required. A monitor with 1280x1024 resolution or higher is recommended.
- Dual monitors are supported.
- Internet access is required during the installation of Working Papers.
- Updates between releases are available as downloads from the CaseWare International Inc. website at [www.caseware.com/support/working-papers](http://www.caseware.com/support/working-papers). A high-speed internet connection is recommended for downloading program updates.
Additional Components - Microsoft Office

- Microsoft Office 2013 (32-bit and 64-bit)
- Microsoft Office 2010 (32-bit and 64-bit)
- Microsoft Office 2007 Service Pack 3 or higher
- Microsoft Office 2003 Service Pack 3*

*On April 8, 2014, Microsoft will end their support for Windows XP and Office 2003. On that date, Windows XP and Office 2003 will no longer be supported for any CaseWare products.

Additional components - Other

- Microsoft Internet Explorer version 8.0 or higher
- Adobe Acrobat Reader version 11.0 or higher

Security and permissions

- Installation requires local administrative rights to the workstation.
- Use of Working Papers requires read/write access to the program folder and any folders containing client files.

SQL Server requirements for SQL Data Store

The Working Papers Data Store can make use of a Microsoft SQL backend to store data. Working Papers 2014 (using a SQL Data Store) is compatible with the following SQL products:

- Microsoft® SQL Server® 2005
- Microsoft® SQL Server™ Express 2005. This is a free version of Microsoft SQL that the Data Store Admin tool will install (if required). The system requirements are as follows:
  
  - Minimum 4 GB hard disk space per database
  - Minimum 1 GB RAM
  - 1 CPU - you can install and run SQL Server on multiprocessor machines, but only 1 CPU is used at any time.

- Microsoft® SQL Server® 2008
- Microsoft® SQL Server® Express 2008
- Microsoft® MSDE 2000 – This version has a limit of eight connections.
1.1.2 File server/networks

A file server can be used to store Working Papers client files.

Operating systems

- Microsoft Windows Server 2012
- Microsoft Windows Server 2008
  
  **Note:** See here for important information when sharing files hosted on Windows Server 2008.

- Microsoft Windows Server 2003 Service Pack 2 or higher
- Microsoft CIFS compatible networks like SAMBA on Linux

Hardware

Per file server/network operating system recommendations.

1.1.3 Windows networking ("Peer-to-Peer")

In situations where a workstation is to be substituted for a true file server, we strongly recommend that the operating system for the workstation be Windows XP Professional (Service Pack 3 or higher). For Windows Vista or Windows 7 users, please refer to the CaseKnowledge article regarding file corruption when using a Windows Vista or Windows 7 workstation or Windows Server 2008 with Server Message Block (SMB2).

Terminal services

A Terminal or Citrix Server can host Working Papers program sessions for users. Requirements include:

- Microsoft Windows Server 2012 with Terminal/Citrix Services
- Microsoft Windows Server 2008 with Terminal/Citrix Services
- Microsoft Windows Server 2003 with Terminal/Citrix Services
- Citrix MetaFrame XP, Presentation Server, XenApp 4.5

Notes

- Server hardware configuration needs to be scaled (RAM, CPU) for the number of sessions to be hosted and the applications and templates used.
- For optimal performance, Working Papers client files should be stored on the Terminal/Citrix Server or connected to it via a high-speed network connection.
2. Overview

Data such as users and file lists are automatically stored in the local computer the first time that CaseWare® Working Papers is launched. This collection of data is contained in private storage, accessible only to the single user, and is referred to as the Personal Data Store.

**Important:** Since the storage is private, there is no way to share user lists between computers if this configuration is used.

Alternatively, a Data Store can be created and accessed on multiple machines. All users connected to the same Data Store have access to a common set of users, global groups, file list, Tracker settings, and store configuration information.

Data Store Administration Tool is a part of the CaseWare Working Papers suite of products. The Data Store Administration Tool enables administrators to create, customize, and maintain Data Stores that will be accessed by multiple users. It is intended for use by an administrator with a fairly high level of IT experience.

**Deciding Whether to Use a Data Store**
Using a Data Store is necessary if one or more of the following hold true:

- You want the protection system on all computers in your firm to have access to a common list of users and global groups.
- You want Tracker on all computers in your firm to have access to a common list of accessed client files.
- You want to use the Active Directory features to populate the user list and to enable Windows authentication.
- You want to use the Security ID feature.

**Note:** If you are upgrading from a previous version of Working Papers, please review the latest Data Store updates.

**Using the Data Store Administration Tool, you will be able to:**

- [Create a Data Store](#)
- [Connect to a Data Store](#)
- [Import users and groups](#)
- [Customize Data Stores](#)
- [Maintain the Data Store](#)
2.1 What's New in the Data Store Administration Tool 2014?
The following major updates have been made to Working Papers' Data Store Administration Tool version 2014.00:

- Active directory integration can now be performed with any LDAP server, not just the default. Radio buttons provide the ability to select the default LDAP server or an alternate using the new fields for the server name and port.
- The hostname control will now accept 260 characters instead of just 15 to accommodate the full hostname length that can be passed to the LDAP server.
- A Find feature has been added to the LDAP dialog and the Protection dialog to use to search for users and groups.
- Resolved an issue with the dialog for the Data Store Admin Tool that prevented it from being minimized.
- Added extra messaging around the Security ID to indicate that it is an optional setting.
- Added a middle name field to the Active Directory Integration dialog and provided the ability to import middle names from LDAP.
2.2 Installing the Data Store Administration Tool

The Data Store Administration Tool is a component separate from Working Papers, which allows you to create, connect to, and customize Data Stores. It is intended for use by an administrator.

The Data Store Administration Tool can be installed on a server or directly onto the administrator's workstation. If installed on the server, the administrator will have to physically log in to the server and run the program from there to perform the actions. A more convenient option is to install the program on his or her own workstation. However, if installing SQL Server or SQL Express Server, the SQL component must be installed on the server.

1. Launch the setup program for the Data Store Administration Tool. The Data Store Administration Tool – InstallShield Wizard launches.
2. On the Welcome screen, click Next.
3. On the License Agreement screen, read the terms, and select the option to accept the terms and click Next.
4. On the Select Options screen, select the Install the Data Store Administration Tool option and/or Install Microsoft SQL Server 2005 Express.

(Note: Only install Microsoft SQL Server 2005 Express if you do not have an existing SQL server installed. If you are installing Microsoft SQL Server 2005 Express, please refer to the Microsoft website for system requirements.)
5. Click Next.
6. Click Install.
2.3 Data Store Best Practices

The best practices in this section all relate to the setup and configuration of the Working Papers Data Store.

- The Data Store should be set up using the Data Store Administration Tool for optimal performance.

- In the Settings tab of the Data Store Administration Tool, ensure that the Synchronization field is set to Only on program startup.

- The Track Engagement field, also in the Settings tab, controls how files are tracked by the Data Store. For these environments, either Track But Do Not Share with Firm or Disable Tracking should be selected in this field. The Track and Share with Firm setting should not be used unless you are using CaseWare Tracker and have a requirement to monitor the files other users are working on as this feature requires increased network bandwidth.

**Note:** Working Papers will frequently ping the Data Store to check its connection status. If one ping fails, the program will stop pinging and the Data Store status icon will remain as a red cross (offline) until you manually reconnect or restart the program.
3. Creation and Connection

3.1 Creating a Data Store

Prerequisites
Before creating a Data Store, ensure that each person who will be attached to the Data Store has read, write, and delete permissions for the directory and server.

Procedure
1. Launch the Data Store Administration Tool.
2. Click the Create/Connect tab.
3. Click Create. The Data Store Creation Wizard opens.
4. Specify the type of store you want to create (either xBase or SQL). Click Next.

- **New xBase Data Store**
  Recommended for smaller offices whose users will be connecting to the Data Store over a reliable fixed wire network.

- **New SQL Data Store**
  Recommended for large offices (more than 50 users) or for any office that has an existing Microsoft SQL Server.

5. Refer to Setting up an xBase Data Store or Setting up a SQL Server Database to continue.
3.1.1 Setting up an xBase Data Store

1. Type in or click **Browse** and navigate to the location where you want the data store to be saved. Click **Next**.

   - To create a new xBase store, enter the folder where you want the store to be created. Either a drive mapped location (i.e., m:\CompanyData) or a UNC (i.e., \sharedserver\store) may be used. It is important that all users who need to attach to the store have full rights (read/write/delete) to the network location.

   If a store already exists at the specified location or if the directory you specified cannot be created, an error message will appear.

   **Important:** Record the location of the newly created store. This location will be required later for other computers connecting to this Data Store.

2. Refer to step 6 of Setting up a SQL Server Database below to finish creating your xBase Data Store.
3.1.2 Setting up a SQL Server Database:

1. Select the SQL product being used to create the tables. The choices are:
   - Microsoft SQL Server 2000
   - Microsoft SQL Server 2005
   - Microsoft SQL Server 2005 Express
   - Microsoft SQL Server 2008
   - Microsoft SQL Server 2008 Express
   - Microsoft SQL Server 2012
   - Microsoft SQL Server 2012 Express

2. Select or enter a server name. The drop-down list contains all available servers on the company network. Select the one on which the SQL databases to be used are located.

3. Enter a unique database name. This database name should indicate that this is a Working Papers database if possible and should follow your organization's standards for database names.

   **Note:** If you are using a SQL database, you must ensure that the Auto Close property for the database is set to False. See [Turning off Auto Close in the SQL Server](#) for more information.
4. Enter the information that you will use to log on to the server. Click **Next**.

Select one of the following options:

- Use Network SQL Server Authentication
- Use Windows Authentication

**Notes:**

- If Windows Authentication is selected, the sup login may not be recognized as administrator. You will need to [add a login in SQL Server Management Studio](#).
- Users who will be performing administration on the SQL store with the Data Store Administration Tool must have db_owner rights. All other users must be granted db_datareader and db_datawriter rights.

5. Specify the server location where the database files will be stored. Click **Next**.

- **The default location for the selected SQL Server (recommended)**
  Select this option to save the SQL Data Store in the default location for the selected SQL server.
- **The following server location**
  Enter the path to the SQL server location.
6. Choose to create a blank Data Store or Import from an existing Data Store.
   
   To create a new and empty Data Store, select **Create a blank Data Store**.
   
   To import data from an existing Data Store, select **Import from existing Data Store**. If you select the **Import Users and Groups** option, you must also provide the import location, the administrator user name, and password.

   **Note:** You can also import users from the **EM database** (Employee database) where all of your employee information can be safely stored.

   - **Import Users and Groups**
     
     Select **Import Users and Groups** if applicable. [See more...]

   - **Import Location**
     
     Provide the import location. Click **Browse** to navigate to a location.

   - **Administrator User Name/Password**
     
     Provide the Administrator User Name and Password.

     **Note:** If you choose not to import Global Groups, references to those groups will be removed from the client files when opened. It is strongly recommended that you import Global Groups if they had previously been set up.
7. Click **Next**. The Choose Database ID screen opens. Creating a Database ID is mandatory.

![Choose Database ID Screen]

**Note:** Record the Database ID. The same Database ID will be needed if the Data Store needs to be re-created for any reason.

8. Click **Next**. The Choose Security ID screen opens. Creating a Security ID is optional.

![Choose Security ID Screen]

**Note:** If specified, record the Security ID. The same Security ID will be needed if the Data Store needs to be re-created for any reason.
9. Click **Next**. The Choose Connection File screen opens. Type in the location or click **Browse** and navigate to a location to save the connection (.cwc) file.

For more information on connection files, please refer to [Creating Connection Files](#).

10. Click **Next**. The Data Store Creation Wizard Complete screen opens.

11. Click **Finish**.

**Results**

All of the information regarding the newly created SQL or xBase Data Store, connection file, Database ID, and Security ID will be displayed.

- If you created an xBase Data Store a .cws file will be created in the location you specified, .cws files point to the location of the Data Store.

- If you created a SQL Data Store, a .cwc file will be created in the location you specified, .cwc files are connection files used to connect/disconnect other users to your Data Store.
3.2 Connecting to a Data Store
Once the Data Store has been created, all computers that require access can be connected to the Data Store.

3.2.1 To connect to an existing Data Store using the program:

1. Launch the Data Store Administration Tool.
2. Click the Create/Connect option.
   You will see the currently connected Data Store and its state, all of which are read-only. If you are not connected to a Data Store, the Data Store field will read “No store currently active.” and the Status will be “N/A”.
   If you are connected to an xBase store, the location of the .cws file as well as its status will be shown. When connected to the store with no errors, the status will be “Online”. When unable to connect to the store (e.g. the store folder is deleted or moved), the status will be “Offline”.
   If you are connected to a SQL store, all SQL connection properties will be shown, along with the status.
3. Click Attach. The Data Store Connection Wizard opens.
4. Select whether you are connecting using the .cwc file, connecting to an xBase store, or connecting to a SQL store. Click Next.

5. Based on your previous selection, perform one of the following:
   a. If you are using an existing connection file (.cwc), enter the location of the .cwc file.
   b. If you are connecting to an xBase store, enter the location of the existing xBase Data Store (.cws file).
   c. If you are connecting to a SQL store, enter all SQL connection information.
6. Click Next.
7. Follow the instructions on the wizard to finish connecting to the Data Store.
3.2.2 To connect to an existing Data Store using the Connection (.cwc) file:

Non-administrators can use the .cwc files created by administrators to connect to or disconnect from Data Stores.

1. Double-click the connection file created by the administrator.
2. Restart Working Papers by closing and re-opening the program.

**Note:** Non-administrator users do not need to install SQL Server or SQL Express to connect to a SQL-based Data Store. The user should have access to the folder where the connection file resides.

3.2.3 To disconnect from a Data Store using a Disconnection (.cwc) file:

1. Double-click the disconnection file created by the administrator.
2. Restart Working Papers by closing and re-opening the program.

**Note:** Ensure your SQL Server is configured to accept remote connections before connecting to a Data Store or else users may experience difficulty connecting to the store. To enable remote connections you need to run the SQL Server Configuration Manager tool (bundled with the SQL Server installation package) and in the section of SQL Server Network Configuration | Protocols for 'Your SQL Instance Name', make sure TCP/IP is enabled.

3.3 Turning off Auto Close in the SQL Server

When you create a Data Store in a SQL Server, you must set the Auto Close property for the SQL database to False. This ensures that the database does not unexpectedly go offline if no one is connected to it.

1. Launch Microsoft SQL Server Management Studio Express.
2. In the Databases folder, locate the database that you created for the Data Store.
3. Right-click the database folder and click Properties.
4. In the Select a page panel, click Options.
5. In the Automatic panel, click the drop-down beside Auto Close. Choose False.
6. Click OK.

3.4 Creating Connection (.cwc) Files

The main purpose of .cwc files is to distribute the Data Store settings to users without administrator rights so that they can connect to or disconnect from a Data Store. The .cwc files can be sent to other users (i.e. non-administrators) who can then use the file to access the Data Store.

To create a .cwc file to connect to a Data Store:

Ensure you are currently attached to a Data Store.

1. Launch the Data Store Administration Tool.
2. Click the Create/Connect option.
3. Click Save.
4. Type in or click Browse and navigate to a location to save the .cwc file.

**Note:** It is recommended that you name the .cwc file "Connection file.cwc" to distinguish it from a disconnecting .cwc file.
To create a .cwc file to disconnect from a Data Store:
Ensure you are currently not attached to a Data Store.

1. Launch the Data Store Administration Tool.
2. Click the Create/Connect option.
3. Click Save.
4. Type in the location or click Browse and navigate to a location to save the .cwc file.

   **Note:** We recommend that you name the .cwc file “Disconnection file.cwc” to distinguish it from a connecting .cwc file.

### 3.5 Create/Connect tab

This tab shows the currently connected store and its state, all of which are read-only.

**Notes:**
- When not connected to a Data Store, the dialog will say "No Data Store currently active" and the status will show as "N/A".
- If connected to an xBase store, then the location of the .cws file as well its status will be shown. When connected to the store with no errors the status will be "Online". When unable to connect to the store, the status will be "Offline" (e.g. if the store folder is deleted or moved).
- If connected to a SQL store, all SQL connection properties will be shown, as well at the status.
- When status is either not connected or "N/A", then all options on all other options will be disabled.
• **Create**
  Launches the Data Store Creation Wizard, which allows you to create a new xBase or SQL store.

• **Attach/Detach**
  If the **Attach** button is shown, then you are not currently connected to a store and this button will allow you to connect to an existing SQL or xBase store. If the **Detach** button is shown, then you are currently connected and this option will simply disconnect you from the store.
  Clicking **Attach** launches the Data Store Connection Wizard.
  **Note:** You can also connect to an existing data store by navigating to the .cwc file on your computer and double-clicking on it.

• **Save**
  Allows you to create a new connection (.cwc) file.
  Specify the location to save the .cwc file and click **Save**.

3.6 **Viewing the status of the Data Store**
Access these options by right clicking the **Data Store** menu within Working Papers.

• **Properties**
  Shows the properties of the data store such as Tracker settings and Data Store information.
  **Note:** This information is the same as the properties shown when selecting **Tools | Options | Data Store** from within a client file or **Options | Data Store** when a client file is not open.

• **Refresh Now**
  Forces the Personal Data Store and Data Store to synchronize. The Data Store icon will change to the synchronization icon for a short period of time and then change back. If not connected to a Data Store, this icon will be grayed out.

• **Connect/Disconnect**
  When connected to a Data Store that is online, selecting **Disconnect** will take the Data Store offline. If connected to a Data Store that is offline, selecting **Connect** will take the Data Store online. The online/offline state of the Data Store will be preserved when you exit and re-open Working Papers. If no Data Store exists, this option will be grayed out.
4. Managing Users

4.1 Populating the User List
When the Data Store is first created, it contains one administrative user, **SUP** with the password **sup** (note lowercase on the password). Subsequent users can be imported in one of the following ways:

- **Active Directory import**
- **Maintenance | Import** option
- For legacy import from previous versions of Working Papers, please refer to [Upgrading from previous versions of Working Papers](#).

**Note:**
- In general, a firm will do an Active Directory import, legacy user list import, or an import through the Maintenance option.
- It is not necessary to import a user list: users may instead be added manually as described in the Working Papers help topic "Creating a new user".

4.2 Connect to Active Directory Server dialog
Administrators will populate the user list used in Working Papers based on their current list of network users. Authentication can be done automatically on opening a client file, based on the current logged in Windows User.

Setting up Active Directory User Authentication and importing from Active Directory is done from **Tools | Options | Data Store**.

When Working Papers cannot find the LDAP server, for example the computer is not connected to a domain or the LDAP server is located on a different domain, the Connect to Active Directory Server dialog opens.

Complete the following information in order to connect to the LDAP server.

- **Host name**
  Type the name of the LDAP server.

- **Port number**
  Type the LDAP port number.

4.3 Importing/Adding users from the Active Directory
Users contained in the Windows Active Directory can be imported into the Working Papers user list. In addition to the user name, extra information such as the user's last name will be brought in.

Using this integration with Active Directory, you can use the same user list for logging in to Working Papers that is used to log in to Windows and your company network. This means a user can have one ID and password that logs him or her in to your firm's network and automatically authenticates the user when he or she logs in to Working Papers.

User accounts added to Working Papers from the Active Directory have restrictions on what can be updated. The first name, last name, and designation fields are grayed out in Working Papers. Information in those fields can be changed only in the Windows Active Directory. After updating, re-import the updated user accounts.
Note:

- The Active Directory Import is available only if a Data Store is being used and if Active Directory Integration is turned on in the Administrator options dialog (Tools | Options | Data Store | Administrator Options).

- The import can only be done from the default Active Directory server. It is possible to import from several Active Directory servers. However, the import for each server must be done from a computer which connects to that server by default.

- Users not assigned to global groups will not have protection rights. You must assign users to a global group with protection rights to enable protection.

4.4 Adding users from the Windows Active Directory
User accounts added to Working Papers from the Active Directory have restrictions on what can be updated. The first name, last name, and designation fields are grayed out in Working Papers. Information in those fields can be changed only in the Windows Active Directory. After updating, re-import the updated user accounts.

1. Enable the Windows Active Directory if it's not already enabled.
2. Click Synchronize with Active Directory.
3. Scroll down the list and check the synchronize box beside each user to add from the Active Directory.
4. As applicable, enter a Default Password for New Users.
5. Select the check box beside Require user to change this password to require users to change the default password to a new one the first time they log in to Working Papers.
6. Click OK to process the additions.
7. Click OK to close the Data Store options.

4.5 Active Directory Import
The Active Directory Import allows users contained in the Windows Active Directory to be imported into the Working Papers user list. In addition to the user name, additional information such as the user’s last name and middle name will be brought in. A user can have one ID and password that logs him or her in to the firm's network and automatically authenticates the user when he or she logs in to Working Papers.

The Data Store can manage users in conjunction with Windows using the LDAP protocol to check the user's login and workstation hostname for logins. In previous versions of Working Papers, the maximum length for the hostname was 15 characters. Since many complex hostnames were too long for this field to accommodate, hostnames up to 260 characters can now be handled when validating Active Directory logins. This change should be able to accommodate almost any required hostname during user login validation.

Note:

- The import can only be done from the default Active Directory server. It is possible to import from several Active Directory servers. However, the import for each server must be done from a computer that connects to that server by default.

- If a Time-integrated Data Store is being used, users are imported as non-Timekeepers for Time. If a user is to be designated as Timekeeper, the user must be explicitly set as such in the Staff dialog in Time.
Prerequisites
Assigning an Active Directory admin user may be useful in the event that you **Allow Active Directory authenticated users only**.

To import users from the Active Directory to your Data Store:

1. Launch the Data Store Administration Tool.
2. Click the **Active Directory** option. You will be required to enter your administrator's login and password.
3. Specify the fields.
   For more information, see **Active Directory**.
4. Click **Synchronize with Active Directory**. The Active Directory Integration screen that appears should display all of the Active Directory users that can be integrated with the Data Store. Select the check box in the Synchronize column for any staff that will have access to Working Papers.

![Active Directory Integration Screen](image)

5. The **Default Offline Password** can also be set on the screen above. This password is shared for all logins and enables users to access the Data Store even if the Active Directory authentication is unavailable. Once you have selected all of the required users and filled in the **Default Offline Password** if required, click **OK** to continue.

**Note:** By default Active Directory will never include disabled users in an LDAP import.
4.6 Active Directory tab
When you are connected to a Data Store, you will need to log in before accessing the Active Directory tab.

- **Enable Active Directory Integration**
  Select this option to enable all other controls in the dialog.

- **Active Directory must be connected to allow authentication**
  If selected, authentication will not be allowed using cached credentials. If Active Directory is not available then users will not be able to log in.

- **Allow Active Directory authenticated users only**
  If selected, the Working Papers option **Tools | Change User** will be disabled and only Active Directory users will be able to log in. If it is not selected then mixed types of users can log in. For more information on this option you can search the Working Papers help for, "Logging in as a different user".

- **Default/Non-Default LDAP Server**
  The default LDAP server that is set up in the Data Store tool is selected by default. To connect to a non-default LDAP server, specify the host name and port.

- **Filter field**
  The administration tool now provides a filter option when importing users with Active Directory Integration. You can specify expressions to filter based on built-in or custom user attributes and Windows group memberships. Wildcards are supported. For more information, see [Using LDAP Import Filters](#).

- **Synchronize with Active Directory**
  Click this button to launch the **Active Directory Integration** dialog.
4.7 Enabling Windows Active Directory

1. Launch the **Tools | Options | Data Store** screen.
2. Click the **Administrator Options** button.
3. Click to check the box beside **Enable Active Directory Integration**.
4. Click **OK** to close the dialog.

4.8 Active Directory Integration dialog

The Data Store can manage users in conjunction with Windows using the LDAP protocol to check the user’s login and workstation hostname for logins. In previous versions of Working Papers, the maximum length for the hostname was 15 characters. Since many complex hostnames were too long for this field to accommodate, hostnames up to 260 characters can now be handled when validating Active Directory logins. This change should be able to accommodate almost any required hostname during user login validation.

**Note:**

- If a Time-integrated Data Store is being used, users are imported as non-Timekeepers for Time. If a user is to be designated as Timekeeper, the user must be explicitly set as such in the Staff dialog in Time.

- **Default Offline Password**
  Check to require a user to enter an offline password when he cannot be authenticated by Active Directory.

- **Import user initials**
  Check the box to import the users’ initials.

- **Import user middle name**
  Check the box to import the users’ middle name.
The following table describes each column in the dialog:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synchronize</strong></td>
<td>Select the <strong>Synchronize</strong> check box beside the Windows users who are to be imported as Working Papers users. Users who had previously been imported will automatically be selected for re-synchronization. This allows Working Papers to update the information for its users (synchronize the information) with the information stored in the Active Directory. <strong>Important:</strong> If the <strong>Synchronize</strong> check box is cleared for a user that had previously been imported from the Active Directory (that is, the user exists in the Active Directory user list and Working Papers' user list), the user is removed from the Working Papers' user list, but remains in the Windows Active Directory.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>To import the user as active, select the <strong>Active</strong> check box beside the user. If the check box is cleared, the user is imported as inactive. Only active users can be assigned to groups.</td>
</tr>
<tr>
<td><strong>Force Password Change</strong></td>
<td>Check the box to require users to change the default password to a new one the first time they log into Working Papers.</td>
</tr>
<tr>
<td><strong>Is Password Set?</strong></td>
<td>This indicates whether a user has a password or not. Use this column to group and sort by users with or without passwords.</td>
</tr>
<tr>
<td><strong>OU Path</strong></td>
<td>The path to the organizational unit.</td>
</tr>
<tr>
<td><strong>OU</strong></td>
<td>The Active Directory organizational unit containing the users and computers managed by the logged in administrator.</td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
<td>The common name (CN) of the user with an account in the Active Directory organizational unit.</td>
</tr>
<tr>
<td><strong>Last name</strong></td>
<td>The last name of the user stored in the Windows Active Directory.</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td>The title of the user stored in the Windows Active Directory.</td>
</tr>
<tr>
<td><strong>Physical Delivery Office Name</strong></td>
<td>The name of the user's office.</td>
</tr>
<tr>
<td><strong>First Name</strong></td>
<td>The first name of the user.</td>
</tr>
<tr>
<td><strong>Department</strong></td>
<td>The department name of the user.</td>
</tr>
<tr>
<td><strong>Company</strong></td>
<td>The company name of the user</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td>The Email address of the user.</td>
</tr>
<tr>
<td><strong>Phone Number</strong></td>
<td>The phone number of the user.</td>
</tr>
<tr>
<td><strong>Cell Phone</strong></td>
<td>The cell phone number of the user.</td>
</tr>
<tr>
<td><strong>Account Name</strong></td>
<td>The account name of the user</td>
</tr>
<tr>
<td><strong>DN (Distinguished Name)</strong></td>
<td>A unique identifier for the user.</td>
</tr>
<tr>
<td><strong>Initials</strong></td>
<td>The initials of the user.</td>
</tr>
<tr>
<td><strong>Middle Name</strong></td>
<td>The middle name of the user.</td>
</tr>
</tbody>
</table>
• **LDAP Find**

In large organizations that use LDAP and Windows Active Directory to manage user access to Working Papers, it can be difficult to locate a particular user or other LDAP object or attribute due to the volume of data involved. Therefore, Working Papers includes a Find function when dealing with LDAP in the Protection and LDAP setup dialog boxes. This dialog box is available through the Ctrl+F hotkey combination in the Protection and LDAP setup dialog boxes.

- The Find what field is used to enter the search term.
- The Where field is used to filter the search for particular kinds of LDAP information such as:
  - Anywhere
  - User ID
  - Group
  - Description
  - Actual Rate
  - Plan Rate
- The Match field can be used to search on Any Text or the Whole Word used in the Find What field.
- The Match Case check box is used to match the character cases used in the search term(s).

In the left pane of the Protection setup dialog box where Users and Global Groups information is contained, Ctrl+A can also be used now to select all entries.

### 4.9 Adding a Login Using SQL Server Management Studio

When Windows Authentication is turned on you must login through the SQL server. If your login is not recognized you will not be able to login. You can add logins to SQL Server Management studio. This is useful when Windows Authentication is turned on for a SQL Data Store.

**Prerequisites**

Ensure SQL Server Management Studio is installed on your machine (bundled with the SQL Server installation package).

**Procedure**

1. Launch SQL Server Management Studio.
2. Login using your credentials. Click **Connect**.
3. Navigate into the folders **Security | Logins**.
4. In the Logins window, right-click and select **New Login**.
5. Specify all of the fields in the Login - New dialog. Click **OK**.

**Results**

Your login has been created. Reattempt logging into Data Store if you were having issues.
4.10 Using LDAP Import Filters
You can use the filter field to customize your Active Directory Import. To use the filter field to customize your Active Directory Import, follow this procedure.

**Note:** The filter field is available when **Enable Active Directory Integration** has been checked.

**Procedure**

1. From the Data Store Administration Tool, click the Active Directory tab. Enter any credentials.
2. In the **Filter** field, enter a filter such as `department=w*` to retrieve all active users in a department that starts with the letter 'w'.

   ![Filter Field Example](image)

3. Click **Synchronize with Active Directory**.

**Results**
The Active Directory Integration dialog opens and all active users in a department that starts with the letter 'w' will be displayed.

**Filter examples:**

- To retrieve users last modified between Jan. 01, 2013 and April 04, 2013 type: `&(whenChanged>=20130101050000.0Z) (whenChanged<=20130402035959.0Z)`
- To retrieve all active users in a department that starts with the letter 'w' type: `(department=w*)`
- To retrieve all active users from the LDAP server type: `(userAccountControl:1.2.840.113556.1.4.803:=2)`
- To retrieve users in some Windows group membership type: `(memberOf=xxx)` - where, xxx, represents the distinguished name of the Windows group
Filter parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-LDAP</td>
<td>Perform LDAP import</td>
</tr>
<tr>
<td>-DP</td>
<td>Default offline password</td>
</tr>
<tr>
<td>-UI</td>
<td>Import user initials</td>
</tr>
<tr>
<td>-MN</td>
<td>Import middle name</td>
</tr>
<tr>
<td>-Filter</td>
<td>(Optional) LDAP filter expression</td>
</tr>
<tr>
<td>-Host</td>
<td>(Optional) LDAP host name</td>
</tr>
<tr>
<td>-Port</td>
<td>(Optional) LDAP port number</td>
</tr>
<tr>
<td>-LU</td>
<td>(Optional) User name</td>
</tr>
<tr>
<td>-LP</td>
<td>(Optional) User password</td>
</tr>
<tr>
<td>-LD</td>
<td>(Optional) Domain name</td>
</tr>
</tbody>
</table>

4.11 Using Command Prompt for Import Filter

Follow this procedure to use command line parameters for your Active Directory Import instead of the filter field.

Procedure

1. In your C: drive, navigate to the Windows | System32 folders.
2. Navigate to cmd.exe. Right click and select Run as Administrator.
3. Enter cd \. Press ENTER.
4. Enter cd program files (x86). Press ENTER.
5. Enter `cd "CaseWare Data Store Administration Tool"`. Press ENTER.

6. Type `sharedstoreadmin.exe` (followed by your customized filter). Press ENTER.

**Results**
The Data Store Administration Tool and the Active Directory Integration dialog opens to begin your import.

**Filter Example**
You can type `SharedStoreAdmin.exe -U sup -P sup -LDAP` (replace `sup` with your username/password) to perform an LDAP import.

In this example, `SharedStoreAdmin` executes Data Store, `-U` and `-P` represent logging on with a username and password and `-LDAP` will perform an LDAP import.

**Note:** If there is a space between parameters you must use quotation marks around the parameters. e.g. Instead of using `SharedStoreAdmin -U sup -P sup -LDAP -filter (department=working papers)`, you must put quotation marks around 'working papers'. The correct syntax is `SharedStoreAdmin -U sup -P sup -LDAP -FILTER (department="working papers")`. 
5. Settings

When you are connected to a Data Store, you will need to log in before accessing the Settings tab. Use this tab to specify custom properties for your file information. Click the Settings tab to access these options.

- **Database ID**

  The Database ID is displayed for informational purposes only and may not be modified. This is set when the Data Store is created.

  The database ID provides a label for the global group database (including information such as the name, rates, security settings, and users) stored in the Data Store. It is set when the Data Store is created. The database ID ensures that global group information maintained in the Data Store is correctly synchronized with client files.

  When the user is connected to the Data Store, the database ID is written into the client file when it is first accessed. Therefore, the synchronization of global group information can only be performed if the database ID contained in the Data Store matches the ID contained in the client file.

  **Note:** The database ID for the Data Store cannot be changed once it is set.
• **Security ID**

If a value has already been set, this is a read-only field and cannot be edited. If it was blank and you enter a value, the field will become read-only.

The security ID feature prevents unauthorized administrative access to a client file that has protection enabled. The security ID may be specified if not previously set. If previously set, it will be displayed for informational purposes only and may not be modified.

As an administrator, you can prevent administrators of other Data Stores from having full access to client files by setting a security ID. The security ID adds another level of protection to the client file; however, you can choose not to set it and allow administrators of other Data Stores to have full administrative access to files.

**Important:** The security ID feature does not affect non-administrators. It only serves to prevent unauthorized administrative access.

• **Synchronization**

Select the frequency at which to synchronize the personal stores with the Data Store. You can choose to synchronize upon startup, every 5, 15, or 30 minutes.

• **Track Engagement**

You can control whether client file access is recorded in the Data Store. The options selected here are then displayed in the **Settings** tab if you want to see the properties that have been set. The choices are:

  • **Disable Tracking**

    If tracking files overburden your computer system’s resources or there is no need to list all client files in Tracker, you can turn off file tracking and sharing by selecting **Disable tracking**. In this case, no file data is processed to either the personal or Data Stores.

    No record of client file access will be made in the Data Store. This is a shared setting that will be used by all users. An individual user may not override this option.

  • **Track But Do Not Share with Firm**

    If you want files to be tracked by the Personal Data Store only, also select **Track But Do Not Share with Firm**. The file information is not shared with others attached to the Data Store.

    Each user will have access to the list of files he or she has accessed. This list will not be accessible to other users in the firm. This is a shared setting that will be used by all users. However, users have an option to override this choice in Working Papers and turn off file tracking altogether in the main **Tools | Options | Data Store** tab.

  • **Track and Share with Firm**

    To track files, select **Track and Share with Firm**. Once selected, files are tracked and shared firm wide. Everyone attached to the same Data Store can view each other’s file information using Tracker.

    All file access is recorded and the list of all users’ file accesses is available to all users. This is a shared setting that will be used by all users. However, users have an option to override this choice in Working Papers and turn off file tracking altogether or to view only their own engagements in the main **Tools | Options | Data Store** tab.
• **Require log in for Tracker**

If this option is selected, users must log in to Tracker when it is opened.

To ensure only users who are administrators can create shared views in Tracker, select the **Require log in for Tracker** check box. When Tracker is opened, the Log In dialog appears. If the **Administrator** check box is selected for the user logging in, then the user has administrative rights to create, copy, modify, or delete shared views. If the **Administrator** check box is cleared for the user, then only personal views can be created, copied, modified, or deleted.

To permit all users to create, copy, modify, or delete shared views, clear the check box.

If both the **Enable Active Directory Integration** check box and the **Require log in for Tracker** check box are selected, then the user is automatically logged in on opening Tracker.

• **Perform log in after client files are uncompressed**

  - If this option is selected, the file will be uncompressed first before the login dialog shows. If you won't provide the correct login credential or simply cancel the login dialog, file will be left uncompressed.
  - If this option is cleared, the login dialog will show up before the file is uncompressed. If the login process does not proceed properly, file will be left compressed.

  **Note:** When converting a compressed 2009 file into a 2010 or higher version, or opening a previously compressed 2010 file, in both cases if the Perform log in after client files are uncompressed option is cleared when the files were compressed, opening these files will always require you to log in first regardless of your current DSAT setting.

• **Use personal store image**

If this option is selected, a personal store image will be created and used. A personal store image is essentially an up-to-date copy of a fully synchronized personal store. Using a personal store image allows for the fast creation of a personal store for new users or for quick updating of personal stores for users already connected to a Data Store. A personal store image reduces the load on a Data Store server.

• **Browse**

If you select the **Use personal store image** option, you will be prompted to enter the location of either an existing personal store image or the location of where you want the image to be created. It is important to enter a path that is accessible by all users who will need to access the image; a shared network location is ideal.

• **Refresh**

From time to time, you may want to update the contents of an existing personal store image. For example, if the contents of a Data Store changes significantly, it is advantageous to create a new personal store image to allow both new users connecting to the Data Store and existing users to quickly receive a fresh synchronized copy of the Data Store. To update a personal store image, click **Refresh**.

**Note:**

- The first time you run Working Papers after a personal store image is created, you will receive a pop-up message stating that the program must be restarted to allow for synchronization of the personal store image. This message will appear only once.
### 5.1 Security ID overview

The security ID feature prevents unauthorized administrative access to a client file that has protection enabled.

As an administrator, you can prevent administrators of other Data Stores from having full access to client files by setting a security ID. The first time a client file is accessed, the security ID of the data store is written into the client file. This ID ensures that only administrators connected to the proper Data Store be granted full access to a particular file. The security ID adds another level of protection to the client file; however, you can choose not to set it and allow administrators of other Data Stores to have full administrative access to files.

The Security ID is set using the Data Store Administration Tool. For more information, see Setting the Security ID.

**Important:** The security ID feature does not affect non-administrators. It only serves to prevent unauthorized administrative access.

#### When a Security ID is set

Once a security ID is set, it is locked to that Data Store. When a client file is first opened by someone connected to the Data Store, the security ID of the Data Store is written into the client file.

If a security ID is set, an administrator may log into a file only if the security ID of the data store matches the security ID of the client file. The security ID matching only occurs if a client file contains a security ID.

If the IDs do not match, a message is displayed indicating that the security ID for the Data Store does not match the security ID of the client file.

The Security ID feature can be disabled to allow administrators connected to a different data store to log into your files.

**Important:** It is not required that the same Data Store that was active when a client file was first accessed be used when subsequently accessing the client file as an Administrator. It is only required that the Security ID remain the same. If the user list in the data store needs to be recreated for any reason, it is then only necessary to re-enter the same ID to have continued access to client files as an administrator. For this reason, it is important that a record of the security ID be made when creating a Data Store.
Copy Components and Security ID
The Working Papers Copy Components function has the following limitations where security IDs are concerned when you are logged in as an administrator:

<table>
<thead>
<tr>
<th>Copy Components</th>
<th>The template is copied.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy all components</td>
<td>The security ID is copied.</td>
</tr>
<tr>
<td>Copy some components to a new file</td>
<td>The template is copied.</td>
</tr>
<tr>
<td>Copy some components to an existing file</td>
<td>The security ID is copied.</td>
</tr>
<tr>
<td>Year End Close and Security ID</td>
<td>The security ID is not copied.</td>
</tr>
</tbody>
</table>

Note the following:

- Where the security ID is set in both the source and destination files, but they do not match, the template is not copied. To copy the template, log in as a non-administrator with copy components rights. You need to log in to both files, so you need to have the appropriate rights for both files. You must also disable the security ID.
- If the source file does not have a security ID and the destination file does, the template is not copied. To copy the template, you can open the file while connected to the same Data Store as the destination file. Alternately you can use a non-administrator login with the appropriate rights.
- If copying from a protected file to an existing unprotected file, the security ID is not copied.

Year End Close and Security ID
If the source file is protected and has a security ID set, that security ID overwrites the security ID of the destination file.
5.2 Setting the Security ID
To prevent unauthorized administrator access to files on a Data Store, an administrator can set a security ID.

**Important:** You must keep a record of the security ID. If the user list in the Data Store needs to be recreated for any reason, the same ID must be entered to have continued access to client files as an administrator.

To set the security ID when creating a Data Store with the Data Store Administration Tool:

- When creating a Data Store, enter a security ID in the **Choose Security ID** page of the Data Store Creation Wizard.

5.3 Disabling the Security ID
When a security ID is set on the Data Store, client files linked to that Data Store cannot be opened by an administrator of a different Data Store.

If you are an administrator of the Data Store, you can disable the security ID. By doing so, the protection-enabled client file can be opened by an administrator connected to a different Data Store.

Once the security ID is disabled and an administrator of a different Data Store opens the client file, the following occurs:

- The **Allow administrators connected to a different data store to log onto this file** check box is cleared.
- The security ID of the new store is linked to the client file and can only be opened with the new Data Store.
- If no security ID exists in the new Data Store, the security ID is removed from the file.

**Note:** The file is maintained under the original Data Store in the following circumstances:

- When a non-administrator connected to a different Data Store opens the client file.
- If the check box is cleared before the file has been opened by an administrator of a new store.

To disable the Security ID:

1. From within a Working Papers client file select **Tools | Protection | Protection Setup**. The Users and Groups dialog opens.
2. Click the **Setup** button. The Setup Dialog opens. Note that you must be logged in as an administrator to access this tab.
3. Select the **Allow administrators connected to a different Data Store to log onto this file** check box.
4. Click **OK**.
6. Maintenance

When you are connected to a Data Store, you will need to log in before accessing the Maintenance tab. Click the **Maintenance** tab to access these options.

- All options, except Resync, are disabled if any shared database is read-only.
- Upon successful completion of any of these operations, a message box will be generated indicating success.

The following buttons are available for the Maintenance option:

- **Resync**
  Forces all users to resync their personal store. The user's Personal Data Store is automatically rebuilt the next time the user is online with the Data Store.

- **Pack**
  Packs the Data Store databases, which also forces a resync of all users. When users, global groups, or engagement file records are deleted, they are marked for deletion and are no longer displayed, but remain in the databases. Selecting **Pack** permanently removes these records from the Data Store databases.

  **Note:** If you select the **Resync** or **Pack** option, the Personal Data Store will not be resynced until you re-open Working Papers, click the **Refresh** button in the status bar, or select **View | Refresh**.

- **Repair**
  Repairs the data store databases.

- **Export**
  Exports the users and groups database to the specified location.

  If you select this option, the **Export Users and Groups** dialog will open.
• Import
Imports users and groups databases from pre-existing Data Stores (Working Papers 2009.00 and lower). You can import old legacy user lists stored in a database file in the program directory.

If you select this option, the Import Users and Groups dialog will open, allowing you to replace the existing list or merge an incoming user list with the existing list.

Note: You can import EM databases.

6.1 Maintenance | Import option
You can also import users and groups using the Maintenance | Import option within the Data Store Administration Tool.

To import users and groups using the Maintenance | Import option:

1. Launch the Data Store Administration Tool.
2. Click the Maintenance option. You will be required to enter your administrator login and password.
3. Select Import. The Import Users and Groups dialog opens.
4. Type in or click Browse to navigate to the folder containing the user/group database you would like to import.
5. Select Preserve passwords if you would like to retain the existing users’ passwords and not have them overwritten by new passwords.
6. Select whether to Merge the source and destination databases or Replace the user/group list in the destination entirely.
7. Click OK.

6.2 Export or Import Users and Groups dialog
Access this dialog by clicking the Maintenance tab | Export or Import.

• Export Users and Groups
Type in the location or click Browse to navigate to the location where you would like to export the users and groups database.
• **Import Users and Groups**
  
  Type in the location or click **Browse** to navigate to the folder containing the users and groups database you would like to import.

  ![Import Users and Groups](image)

  **Select Update Options:**

  • **Merge source users and groups (new users and groups are added)**
    
    Selecting this option will combine the original user list with the imported user list. The process will examine the incoming user names and either append them to the existing user list, or update the list of existing users.
    
    **Note:** This process will not delete existing records.

  • **Replace with source users and groups**
    
    Selecting this option will replace the original user list with the imported user list. If the currently logged in user is not present in the import file, the current user's record will still remain in the database.

  • **Preserve passwords**
    
    If importing, select this option to import the hash value of user passwords.

**6.3 Working Papers Databases**

These are some of the key databases available in Working Papers:

- **Trial Balance/ Financials (AM)**
- **Journal Entries**
- **Account Mapping**
- **Document Manager**
- **Employee Database (EM)**

For a complete listing of databases, see [Database files](#).

**6.4 Database files**

Files with the file name extension DBF are database files. DBF files store the data for the Working Papers client. For example, the AM.DBF file contains account information (i.e., account numbers, descriptions, ratio classes etc.) for a client's working trial balance.

**Note:** Windows XP offline file support cannot be used with Working Papers as DBF files are not supported for offline synchronization.
7. Advanced Options and Troubleshooting

7.1 Overview
This section is meant to provide you with detailed background knowledge for the CaseWare® Working Papers Data Store; how it operates, its requirements and how to repair the Data Store if an error occurs.

**Note:** This documentation contains information for all features of the Working Papers Data Store, some of which may not have been released for your specific region.

It is important to note that in version 2009, the term "Shared Data Store" was replaced by "Data Store". The term "Personal Data Store" still refers to data such as users and file lists that are contained in private storage, accessible only to the single user.

The Data Store is meant to be, for each user, a central location for certain types of information. Information that is stored in the Data Store comprises:

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File meta data</td>
<td>Stores information about Working Papers files such as location, version information, compression state as well as meta data related to each file.</td>
</tr>
<tr>
<td>Security users</td>
<td>Stores list of users available for use in Working Papers security.</td>
</tr>
<tr>
<td>Security groups</td>
<td>Stores Global group information; group properties and user assignment to these groups.</td>
</tr>
<tr>
<td>Shared settings</td>
<td>Stores Data Store configuration information. Ex. Database GUID, security ID, file tracking settings</td>
</tr>
<tr>
<td>Local Settings</td>
<td>Stores information about the state of the Personal Data Store such as the last time the store was synced and against which Data Store (Personal Data Store Only).</td>
</tr>
</tbody>
</table>

Other than Local Settings, which is contained only in a Personal Data Store, the above information will be contained in both the Personal Data Store and the Data Store. If the user has specified a Data Store, then the information will be synchronized between the user's Personal Data Store and the Data Store. If multiple users connect to the same Data Store, then the information will be synchronized between all connected users.

The Personal Data Store is contained within a folder called `C:\Users\<user account name>\AppData\Local\CaseWare`. The files within this folder are stored as xBase database files. The Data Store is either contained in a SQL database if an SQL Data Store is being used or in a “Data Store” Windows folder if an xBase Store is being used. The table names are as follows:

<table>
<thead>
<tr>
<th>File(s)</th>
<th>Personal Store</th>
<th>Data Store (xBase)</th>
<th>Data Store (SQL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>File meta data</td>
<td>files.dbf</td>
<td>files.dbf</td>
<td>TrackedFiles</td>
</tr>
<tr>
<td>Terminology</td>
<td>terms.dbf</td>
<td>terms.dbf</td>
<td>Terminology</td>
</tr>
<tr>
<td>Security users</td>
<td>users.dbf</td>
<td>users.dbf</td>
<td>Employees</td>
</tr>
<tr>
<td>Security groups</td>
<td>groups.dbf</td>
<td>groups.dbf</td>
<td>SecurityGroups</td>
</tr>
<tr>
<td>Shared settings</td>
<td>shprefs.dbf</td>
<td>shprefs.dbf</td>
<td>SharedSettings</td>
</tr>
<tr>
<td>Local Settings</td>
<td>prefs.dbf</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Addition file. Points to the location of the Data store.</td>
<td>storeinfo.cws</td>
<td>storeinfo.cws</td>
<td>n/a</td>
</tr>
</tbody>
</table>
By default the Data Store always uses the Personal Data Store to retrieve any information because it should always contain accurate information due to synchronization (except when the Data Store is offline, in which case information will become stale as expected) and it is always guaranteed to be online.

To ensure a correct and up-to-date list of client files, always manipulate a client file using Working Papers. For example, use File | New or File | Copy Components to create a new client file rather than copying the file through Windows Explorer.

7.2 Software Environment

The following illustration shows two Data Stores running and both are connected to the same online Data Store. Store 1 is requesting information from the Data Store which will then retrieve it from the Personal Data Store (in most cases) because the Personal Data Store is always considered to be synchronized with the Data Store.

Synchronization between the Personal Data Store and Data Store takes a variable amount of time depending on the size of the databases and how out-of-date the Personal Data Store is.

Unlike all other operations the Data Store does not queue other requests (such as requesting an ICWCentralStoreFileInfo through the GetFileInformation() method) during synchronization, which means it is possible to request information that is not synchronized.

7.3 Lifecycle

The order of events for the Data Store is as follows. The following assumes that the Data Store has already been set up and configured. For Data Store setup, please refer to DataStore.pdf in the CaseWare® Data Store Administration Tool directory.

1. A CaseWare application (e.g. Working Papers, Tracker, etc.) is launched; this will automatically connect to the Data Store.
2. The Data Store will try to create the Personal Data Store if it does not already exist.
3. If anything goes wrong, the Data Store will put itself in the Disabled state (Disabled). To determine what is wrong, navigate to the Tools | Options | Data Store dialog.
4. If there is only a Personal Data Store and it was successfully created, the Data Store will enter the Enabled state (Enabled). Skip to 7.
5. If the Data Store is available then the Data Store will enter the Online state (\(\text{\textbullet}\)) followed by the Synchronizing state (\(\text{\textbullet}\)) and once synchronization is complete the Online state again. If the Data Store is not available then it will immediately enter the Offline state (\(\text{\textbullet}\)).

6. The Data Store periodically monitors the availability of the Data Store (if specified) and if it changes, the current state of the Data Store will be modified.

7. Once all the applications using the Data Store are exited, all connections to the Data Store will be closed.

7.4 Registry

The initialization of the Data Store is primarily controlled by the following registry key and its children (described later on):

- **HKEY_CURRENT_USER\Software\CaseWare International\Data Store**

The Personal Data Store and Data Store settings are saved in the following registry keys, respectively:

- **HKEY_CURRENT_USER\Software\CaseWare International\Data Store\Personal Store**
- **HKEY_CURRENT_USER\Software\CaseWare International\Data Store\Shared Store**

Each registry type can have the following values:

<table>
<thead>
<tr>
<th>Type</th>
<th>Registry Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Data Store</td>
<td>Class</td>
<td>Constant. Must have the value {ea56dd50-b33d-460c-9326-78da507e4f11}</td>
</tr>
<tr>
<td></td>
<td>COM Class</td>
<td>{a55fcf6b-3982-475b-86ad-8ca1e955e9c9}</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Personal Data Store</td>
</tr>
<tr>
<td></td>
<td>Parameters</td>
<td>The parameters used to create the Data Store. Typically this will be:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C:\Users&lt;user account name&gt;\AppData\Local\CaseWare Data Store</td>
</tr>
<tr>
<td>Data Store</td>
<td>PATH</td>
<td>Path to the Data Store not including the “Data Store&quot; part</td>
</tr>
<tr>
<td>(xBase)</td>
<td>StorageType</td>
<td>2 (xBase)</td>
</tr>
<tr>
<td>Data Store</td>
<td>Database Name</td>
<td>Name of the Data Store database on the SQL server</td>
</tr>
<tr>
<td>(SQL)</td>
<td>Password</td>
<td>Encrypted password to the SQL store</td>
</tr>
<tr>
<td></td>
<td>Product Type</td>
<td>Type of SQL server</td>
</tr>
<tr>
<td></td>
<td>Server Name</td>
<td>Name of SQL server</td>
</tr>
<tr>
<td></td>
<td>StorageType</td>
<td>1 (SQL)</td>
</tr>
<tr>
<td></td>
<td>Use Windows Authentication</td>
<td>0 - use SQL authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1- use Windows authentication</td>
</tr>
<tr>
<td></td>
<td>User Id</td>
<td>Encrypted SQL user ID</td>
</tr>
</tbody>
</table>

The standard procedure for users to connect to a Data Store is to use a connection file (.cwc). The connection file is described in the Data Store Administration Tool document.
However, some firms may want to have users connect to a Data store by pushing down the registry keys for the Data Store to each user. The recommended way to do this is to copy the registry keys from the administrator of the Data Store:

1. Launch the Data Store Administration Tool. Ensure that the administrator is pointing to a Data Store. Create a Data Store if required.
2. Run regedit.exe. Find the key HKEY_CURRENT_USER\Software\CaseWare International\Data Store\Shared Store. Right click on the key and select “Export” from the context menu. The resultant .reg file may be pushed down to users (for example in a windows login script).

The Registry and Citrix
This registry information is particularly useful for installations of the Data Store on a Citrix server. After installation of the software is complete, locate the top level branch of the registry HKEY_CURRENT_USER\Software\CaseWare International\Data Store. This can then be pushed to each user’s registry through a login script or copied to the shadow directory. The CaseWare Best Practices for Citrix and Terminal Server guide for here should be consulted for all Citrix implementations of Working Papers.

7.5 Folder Security
The Personal Data Stores and Data Stores always reside in a folder called “Data Store”. Note that in Working Papers version 2008 and lower, the folder was named “Store”. All users have a Personal Data Store usually located (although this can be different depending on the operating system) in the following folder:

C:\Users\<user account name>\AppData\Local\CaseWare

- **For xBase Stores**
  The Data Store should be placed in a location such as a network file server that is accessible to all users who will need to connect to it. All users using the Data Store must have sufficient permissions to create, read, and write to the Data Store folder. In addition, the parent folder must have sufficient permissions to allow the Data Store to create the Data Store’s Data Store folder.

- **For SQL Stores**
  The SQL server must be accessible by all users who will be using the store. We recommend that the server be on the same Windows domain as users who will be accessing the store. If Windows Server Authentication is being used, the database administrator must grant access to all Windows domain users that will be connecting to the Data Store.

7.6 Backing Up
It is recommended that you keep a regular backup (once a week) of the Data Store. The backup method depends on whether an xBase or an SQL Data Store is being used.

For xBase stores, ideally the backup solution would obtain an exclusive lock on all the files in the Store folder to ensure that the database indexes and memo fields are consistent with the database. Working Papers and Tracker only open database files when needed (ie. when idle, no open connections to databases are maintained). However, in a large firm, it may be difficult to time the backup while no user is accessing the Data Store. For this reason, we recommend that the backup be timed to occur when it is unlikely that users will be actively accessing the store (at 3am for example).
For SQL stores, we recommend that the normally installed SQL administration tools (ex. SQL Server Management Studio) be used to perform the backup. Although it is possible to create a backup at any time using SQL, we recommend again to perform the backup it is unlikely that users will be actively accessing the store.

**Restoring**
The method for restoring from backup depends on the type of store involved. Restoring from an xBase backup simply requires all the files in the Store folder to be replaced by the backed up files. This can only be performed when no users are actively accessing the store. If it is suspected that the indexes are out of date, Data Store Maintenance application can be run (see next section).

We recommend that the normally installed SQL administration tools (e.g. SQL Server Management Studio) be used to perform a restore of SQL Data Stores. [See more...](http://technet.microsoft.com/en-us/library/ms187048.aspx)


### 7.7 Maintenance
There are two tools that can be used for Data Store Maintenance; CWMaintenance.exe for Personal Data Stores and the CaseWare® Data Store Administration Tool (SharedStoreAdmin.exe) for Data Stores.

**CWMaintenance.exe**
We recommend to run CWMaintenance.exe periodically to ensure the indexes are correct (for performance) and to pack the databases to remove deleted records and keep their sizes down. There are three operations that can be performed with CWMaintenance:

- **Sync Personal Data Store from Data Store**
  Forces the Personal Data Store to be immediately refreshed with all information in the Data Store.

- **Pack Personal Data Store databases, will force a sync**
  Ensures that unused records in the Personal Data Store are physically removed. This operation will also force a resync to occur.

- **The “Index” operation**
  Ensures that index files used to perform database lookups in the Personal Data Store are correct and up-to-date.

CWMaintenance.exe accepts command line parameters to allow for automated maintenance of a Data Store; if these parameters are used, no interface is brought up and the operations proceed silently. The following two operations can be performed:

- **CWMaintenance /r** forces a personal store to be re-indexed.
- **CWMaintenance /p** forces a personal store to be packed
CaseWare® Data Store Administration Tool
There are five maintenance operations that can be performed on a Data Store. We recommend to perform the maintenance when it is unlikely that users will be actively accessing the store. The operations can be accessed in the Maintenance tab of the Data Store Administration Tool:

- **Resync**
  Forces all users to resync their Personal Data Stores with information stored in the Data Store the next time they run Working Papers or Tracker.

- **Pack**
  Ensures that unused information in the Data Store (i.e. records marked as deleted) are physically removed from the store.

- **Repair**
  Ensures that index files used for database lookups are correct.

- **Export/Import**
  The Export and Import functions are not actual repair methods. They are methods that allow for the import and export of users and group data. Their functions are described in the Data Store Administration Tool document.
7.8 Making the Data Store Read-Only
Making the Data Store read-only has been found to prevent any corruption in an xBase Data Store. Setting a Data Store to read-only is not applicable to SQL stores.

Prerequisites
Ensure that everyone in the firm is not using the Data Store.

Procedure
1. Navigate to the Data Store folder in the location the store was created.
2. Select all the files except the .cws, .bin and .clg files.
3. Right-click on one of the files and select Properties.
4. Select the Read-only check box and click OK.

Results
Making the Data Store read-only will have the following side effects since no data will be able to be written to the databases:

- File tracking will be partially disabled. For example, if a user creates a new client file on their hard drive they will be able to see it in Tracker, but other users connected to the same Data Store will not (unless they specifically open it on their computer).
- Users and groups will not be modifiable; adding, modifying, or deleting will not be possible. Assignment of users and groups to client files will still function correctly.

Setting a Data Store to be read-only can also be performed using Windows Security. This can allow an administrator to retain full access and write to the Data Store (to create new users and groups for example) while write permission can be denied for normal users.
7.9 File Tracking

File tracking refers to the Data Store’s ability to collect metadata information about Working Papers engagement files.

The collection and distribution of this data can be very network bandwidth intensive. For this reason, it may be desirable to not write this information to the Data Store or, if a firm does not use Tracker, to totally disable file tracking altogether. These options can be set in the settings tab of the Data Store Administration Tool:

- **Disable Tracker**
  No information about accessed Working Papers files is recorded. This setting is recommended if a firm does not use Tracker.

- **Track But Do Not Share with Firm**
  Each user's personal Working Papers file access is recorded locally on each machine. However, this information is not written to the Data Store eliminating network bandwidth. In Tracker, each user will be able to see the list of files he or she has accessed, but not the list of files other users have accessed.

- **Track and Share with Firm**
  Each user's personal Working Papers file access is recorded locally on each machine and to the Data Store; as such it is the most network intensive setting. In Tracker, each user will be able to see the list of files he or she has accessed as well as all files other users have accessed.
Each user may choose to lower the level of file tracking used. For example, if file tracking is set to **Track But Do Not Share with Firm** in the Data Store, the user may set file tracking to **Disabled**. This can be set in the “Data Store” tab of the **Tools | Options** dialog in Working Papers. Note that it is not possible for a user to increase the level of file tracking that is set in the Data Store. For example, if file tracking is set to **Track But Do Not Share with Firm**, it is not possible for a user to track “All Engagements” (for all users).

<table>
<thead>
<tr>
<th>User Setting</th>
<th>Disable Tracking</th>
<th>Track but do not share with firm</th>
<th>Track and Share and Firm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disabled</strong></td>
<td>File tracking disabled.</td>
<td>File tracking disabled.</td>
<td>File tracking disabled</td>
</tr>
<tr>
<td><strong>My Engagements</strong></td>
<td>N/A</td>
<td>User's own files tracked but not written to the Data Store</td>
<td>User's own files tracked, but not written to the Data Store</td>
</tr>
<tr>
<td><strong>All Engagements</strong></td>
<td>N/A</td>
<td>N/A</td>
<td>User's own files tracked and written to the Data Store</td>
</tr>
</tbody>
</table>
7.10 Troubleshooting
This page provides documentation for issues and advisories that have been noted and have solutions.

Virus Scanners

- **PROBLEM**
  It is possible that a virus scanner can cause problems when it tries to access the Data Store due to additional file locking issues.

- **SOLUTION**
  Therefore, we recommend, especially for large firms, to exclude the files contained within the Data Store folder from examination by the virus scanner.

  **Note:** The Data Store folder refers to the folder in the location where the store was created.

Corruption

- **PROBLEM**
  Under some circumstances a firm’s Data Store can become corrupted frequently, causing the Data Store to report errors.

  Frequent corruption is generally caused by having a large number of users connected to the same Data Store using a network with low bandwidth and/or frequent network losses (dropouts).

- **SOLUTION**
  The two general solutions are to limit the amount of bandwidth and disk access the Data Store has, or to make the Data Store read-only. To limit the bandwidth the Data Store uses please see the section Low Bandwidth.

Low Bandwidth

- **PROBLEM**
  The Data Store performs poorly in low bandwidth environments.

- **SOLUTION**
  Disable File Tracking.
8. Upgrading from previous versions of Working Papers

All administrative options for Data Stores (previously referred to as "Shared Data Store") are now performed using the new Data Store Administration Tool. In Working Papers, the **Tools | Options | Data Store** dialog simply displays the Data Store settings. When users first install Working Papers, the Data Store settings will remain blank until Working Papers is connected to a Data Store.

Users can now select either an xBase Data Store (as used in Working Papers 2008.00 and prior) or a SQL Data Store. Data Stores from previous versions of Working Papers are not automatically converted. You can convert your Data Store to a newer version without losing any information when installing new versions.

**Note:** Integration to Time using the Time-integrated Data Store functionality is disabled in Working Papers.

Prior to upgrading everyone in the firm to the latest version of Working Papers, we recommend that one user (i.e., an administrator) upgrade existing Data Stores to the new Data Store.

Upgrading Data Stores involves the following steps:

- Create a new Data Store
- Populate the User List
- Create connection files

To upgrade everyone in the firm to use the new Data Store, distribute the connection files along with Working Papers.

**Note:** Data Store Administration Tool is compatible with previous versions of Working Papers. Previous versions of Working Papers are also compatible with previous versions of the Data Store Administration Tool.
9. Getting Technical Support

The CaseWare Support Network offers you a wide range of choices and access to high-quality, responsive technical support.

Before contacting Technical Support, please consult the online Help and any other documentation included with this package as your first source to solve the problem. Be sure to also check the CaseWare website for the latest troubleshooting and technical information.

If you are unable to find the solution, you can receive information about obtaining CaseWare® Technical Support by contacting your nearest CaseWare distributor.

What you need to tell us
When you contact CaseWare® Technical Support, you should be at your computer and have your documentation at hand. Be prepared to provide the following information:

1. Your Client Number.
2. The product version number, found by clicking the Help menu and selecting About.
3. The type of computer hardware you are using.
4. The software version number of MS-Windows.
5. The exact wording of any messages that appear on your screen.
6. A description of what happened and what you were doing when the problem occurred.
7. A description of how you tried to solve the problem.

Contact us
Comments and suggestions about our software and this manual are greatly appreciated. As a user of our products, you are in a unique position to provide ideas that have an impact on future releases of this and other products. You can contact our support teams in several ways to provide your comments. Contact information for CaseWare Support for your country can be found on our website at http://www.caseware.com/about-us/distributors.