WERTHEIM GLOBAL SOLUTIONS, LLC

WINCWALL FOR OPEN TEXT EDOCS™
Installation and Operations Manual

Table of Contents

Introduction

Welcome to WincWall!

WincWall is a companion utility to WincTools which provides the ability to automatically assign security to documents based on any combination of profile criteria. WincWall thus provides an *ethical wall* for your enterprise.

Like WincTools, WincWall is written using the OpenText DM Extensions API calls to perform all functions. This means that WincWall functions regardless of database and Network Operating System (NOS) platforms, and can even support libraries that are running on different database systems.

The WincTools readme.txt file contains information on the latest features, functions and bug fixes in WincTools and companion products. It is suggested that your review the WincTools readme.txt file before attempting to install, run, or upgrade an existing copy of WincTools or WincWall.

System Requirements

WincWall has been tested and operates using the following minimum configurations:

1. Any workstation or server that supports OpenText eDOCS DM Extensions version 5.3.1 or later.
2. A MAPI-compliant email client must be installed on the workstation in order to use WincMonitor.

Notice to Evaluation Users

You are allowed to use WincWall for evaluation purposes for a period of 60 days from the program date, 30 days from the date of installation, or for 15 executions, whichever comes first. Unless you register this program, WincWall will cease to function after the expiration of the evaluation period. A maximum of 10 documents can be secured per session.

WincWall Installation

Initial Workstation Installation

To install WincWall, follow these instructions:

1. Insert the WincTools CD into the appropriate drive of the computer.

2. Navigate to the WincTools eDOCS Version Modules directory, and locate the WincWall directory.

3. Double-click **Setup.exe**, located in the WincWall directory. The following screen will be displayed:

> **Note:** In some cases, the files being copied already exist and are in use. The setup program will need to reboot in order to update these files; if this is the case, you will be informed by the setup application and asked to reboot. After rebooting, follow the steps above once again to return to this point in the installation.

4. The following screen will be displayed; click **OK** to continue.

5. You are now ready to install WincWall. You may change the installation directory if desired, or simply click on the computer icon to begin installation. Note that the installation directory must be the same as the WincTools directory if you are installing both applications on the same workstation.

6. Follow any on-screen prompts to complete the installation. A program group will be created automatically, and a shortcut to the application will be added to your programs folder.

Upgrading an Existing WincWall Installation

Wertheim Global Solutions periodically releases updated versions of WincTools and its associated add-on modules. All updates are released in ZIP (compressed) format, requiring the use of a de-compression program such as WinZip® to decompress the file or files.

In most instances product updates do not require a re-installation of the product. Installation of the update simply requires that the new executable (e.g., WincWall.exe) be extracted to the WincTools installation directory, overwriting the older version.

Updates to our products are made available from the Wertheim Global Solutions website. Visit www.WertheimGlobal.com and click on **Support**. *

To upgrade WincWall:

1. Exit WincTools and all companion products.

2. Open the update ZIP file using a decompression application such as WinZip.

3. Extract all of the files included in the update ZIP file to your WincWall installation directory. For a default installation, this will be C:\Program Files (x86)\Winc.

The WincWall upgrade is then complete.

WincWall Registration

Before you can use WincWall, you will need to enter your serial number. If WincTools is installed on the same workstation as WincWall, you can register via WincTools:

1. Launch WincTools, then choose **Setup Program** from the **Setup** menu:
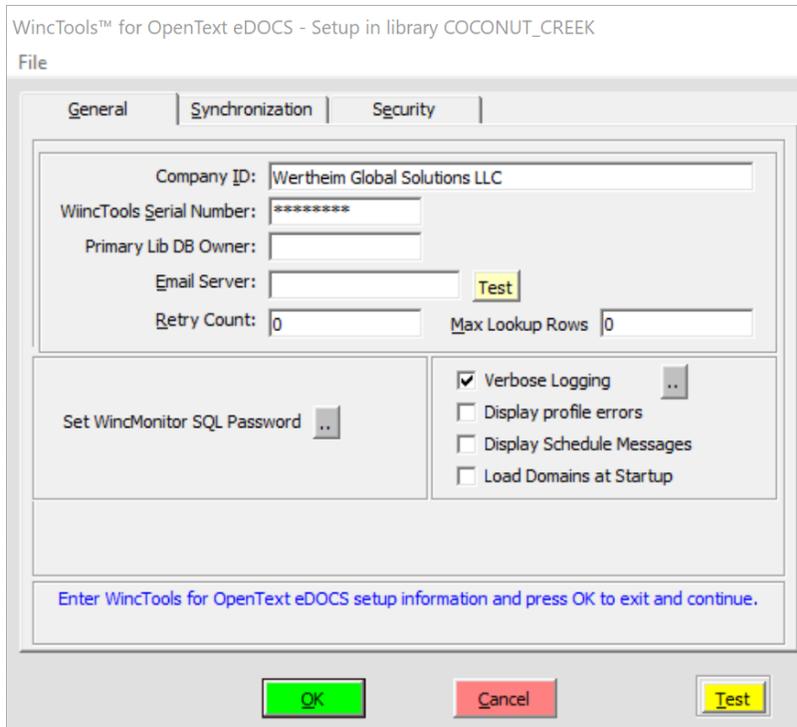
2. Enter the appropriate Company ID and Serial Number. Please refer to the WincTools installation manual for further details regarding WincTools configuration options.

If WincWall is installed alone, you will be asked for the serial number upon launching WincWall:

Configuring WincWall

The WincWall setup process creates a number of tables, if they do not already exist. These include WINC_SETTINGS, WINCWALL_LINK, WINC_SECURITY, WINC_PROXY, and NEEDS_SECURING in each library in which ethical walls will be configured. A trigger is created on the PROFILE table in each of the configured libraries as well; the information gathered when the trigger is executed is placed into the NEEDS_SECURING table.

Upon installation, the trigger immediately begins to place documents into the NEEDS_SECURING table; these documents will wait in the table until walls are created and the WincWall program starts running (see below).

When WincWall finds that a profile has been added to the NEEDS_SECURING table, it performs the requested security operations. This will include setting profile security and network security if appropriate. WincWall will not attempt to set network security if the document server is defined as Generic, Standalone, or DSA, or if the network security option is not enabled in the library's system parameters. For further details on specific security options, please see the WincWall Options beginning on page 9.

Setting up WincWall Tables and Triggers

> **NOTE: If you are also using WincArchive in your enterprise, we strongly recommend contacting Wertheim Global Solutions technical support for assistance with WincWall installation or removal.**

Note: You must be logged into your library's database with the DOCSADM account before proceeding.

- From WincWall go to menu option **Setup | Initial Setup | Setup a Library**.

- If you have more than one library, the following screen will appear. Select the library into which you are setting up WincWall, then click **Yes** to begin installing WincWall to the selected library.
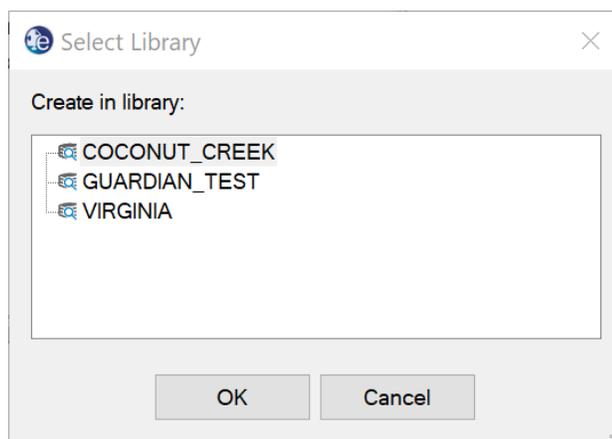
- The following message box will inform you when the WincWall setup is complete. Click **OK**, and check the WincTools error log before proceeding to confirm that setup completed correctly.

-
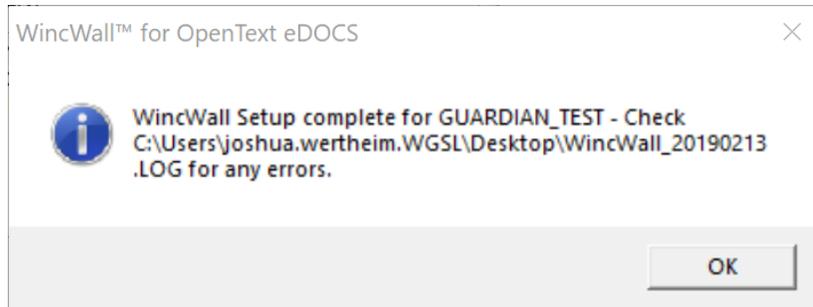
Re-Install Triggers

You may re-install the triggers at any time by selecting **Setup | Initial Setup | Re-Install Triggers** in WincWall. This may occasionally be necessary when updates to WincWall are released.

Removing WincWall

To remove the WincWall table and trigger from your library, go to **Setup | Initial Setup | Remove a Library** in WincWall. You will be asked to confirm.
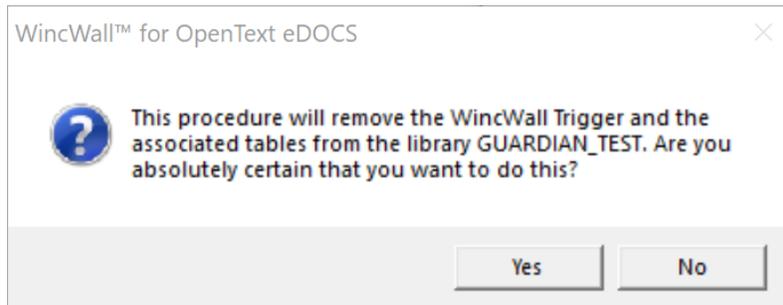
You will be given the opportunity to remove WincWall from all libraries simultaneously.
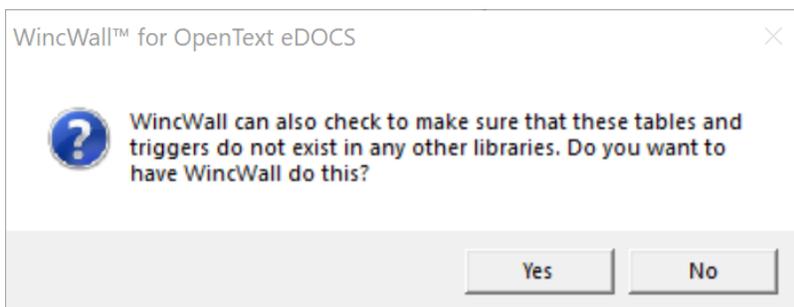
WincWall Application Options

General tab

- **Loop Continuously**: Select this option to have WincWall continuously poll for new or modified profiles to be processed.

- **Delay Time**: Enter the number of seconds to pause between each processing loop.

- **Verbose Logging**: Select this option to have WincWall log everything. It is recommended that this option be left off unless necessary for debugging, as it will adversely affect performance. You may specify a log file name and location by clicking on the ellipses (…) button. Note that all errors will be logged regardless of the Verbose Logging setting.

- **Retry Count**: If left to 0, WincWall will attempt indefinitely to secure any documents which have failed to process.

- **Display Errors**: This option will display a message box any time errors are encountered. This should only be checked for troubleshooting operations, as it will interfere with the continuous operation of WincWall. Will required intervention to continue.

- **Batch Size**: Enter the size of each batch of documents to process per cycle.

- **Process Descending**. Selecting this option will process in descending order by document number; not selecting this option will process the documents in ascending document number order.

- **Lock on Go**! Selecting this option means that when the Go button is pressed to launch WincWall, the Windows login screen will be displayed, so that the computer an be left unattended while WincWall is running.

Options tab
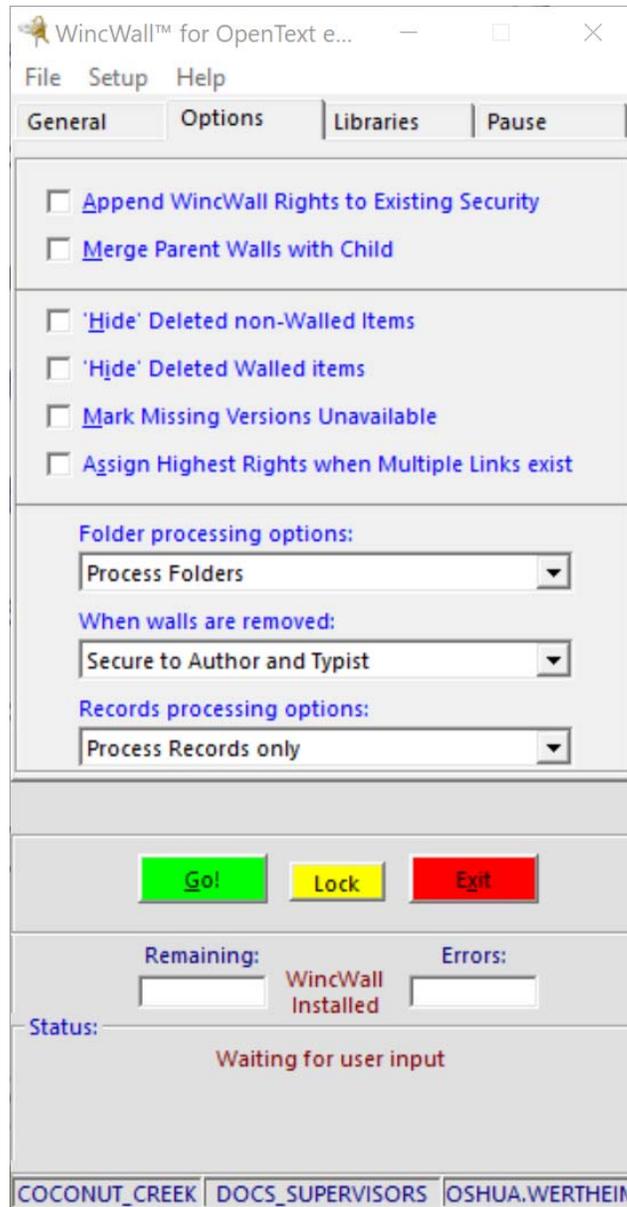
- **Append WincWall Rights to Existing Security**: This option leaves any user-specified security intact and adds configured WincWall security to the document's ACL. If unchecked, the security of the document will be entirely replaced by the security specified in the Wall, including Typist and Author. If you want to keep the rights for Typist/Author you need to add Tokens to the wall as explained on page 19. Note that this becomes the Default value for WincWall to use if it isn't overridden in a wall.

- **Merge Parent Walls with Child (otherwise, override)**: Checking this option will have Parent (i.e. Client) Walls merge with children (i.e. Matter). Note that this becomes the Default value for WincWall to use if it isn't overridden in a wall.

- **Hide Deleted non-Walled Documents**: WincWall provides the option to secure documents marked for deletion so that they don't appear on User's Search Results and are not visible for editing until the actual deletion takes place. This option will secure documents with a storage type of Delete that do NOT have a Wall to Groups that have a UNIV_ACCESS setting of zero (0).

- **Hide Deleted Walled Documents**: WincWall provides the option to secure documents marked for deletion so that they don't appear on User's Search Results and are not visible for editing until the actual deletion takes place. This option will secure documents with a storage type of Delete that DO have a Wall to Groups that have a UNIV_ACCESS setting of zero (0).

- **Mark Missing Versions Unavailable**: If WincWall finds that a document's version does not exist or is zero bytes, it can mark the version row as unavailable (status = 4). This is performed on the version row rather than the profile so that the process of securing the physical file(s) will not fail if network security is enabled on the library.

- **Assign Highest Rights to Trustees with Multiple Links**: With this option checked, a trustee with multiple assignments (e.g., person & group) will be assigned the most permissive security specified. If this option is left un-checked, the trustee will be assigned the most restrictive security specified.

- **Remove Security when Wall is Removed**: Resets the security of documents to their original value when the Wall is removed.

- **Folder Processing Options:** This will determine what to do when a folder profile is encountered. The choices are Process Folders; Do not process DMFolders; or Do not process any folders.

- **When walls are removed**: This will determine what do do with documents that were in a wall, when that wall is removed. The choices are Do not remove security; Remove deny rights; Secure to Author and Typist; or Remove all security.

- **Records processing option**: This will determine what do with records and file parts when eDOCS RM is installed. The choices are Process records and file parts; Process records only; or Do not process any records.

Libraries tab
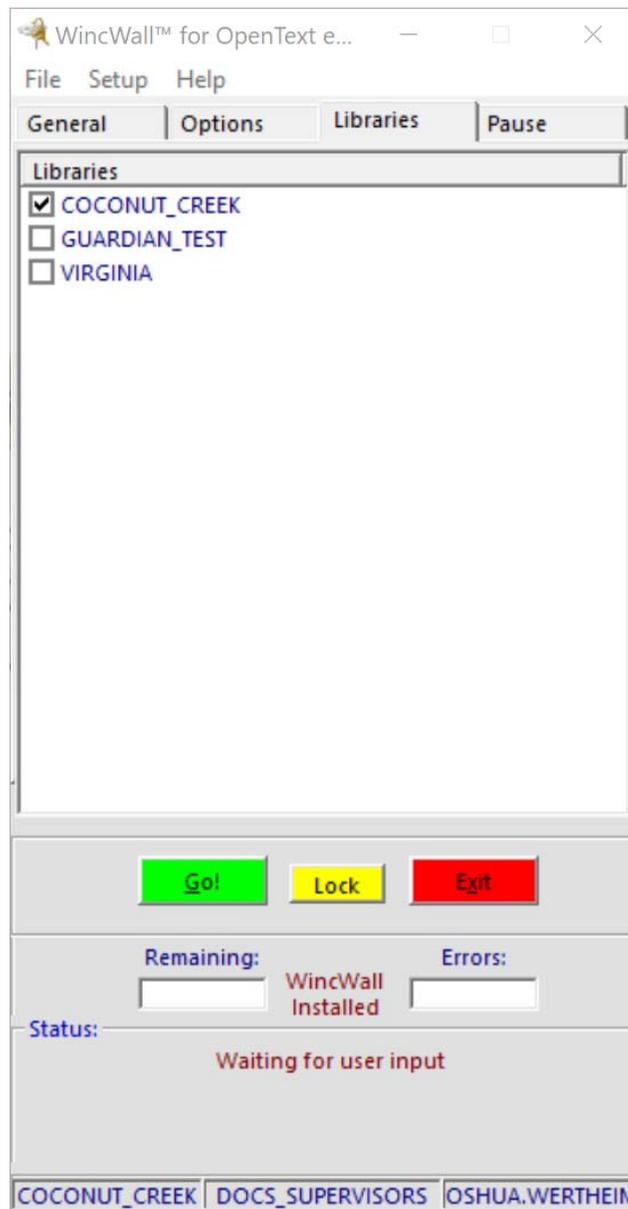
3. On the **Libraries** tab, place a checkmark next to the libraries to be processed by WincWall. Note that the WincWall triggers need to be installed on each library prior to processing.

Pause tab
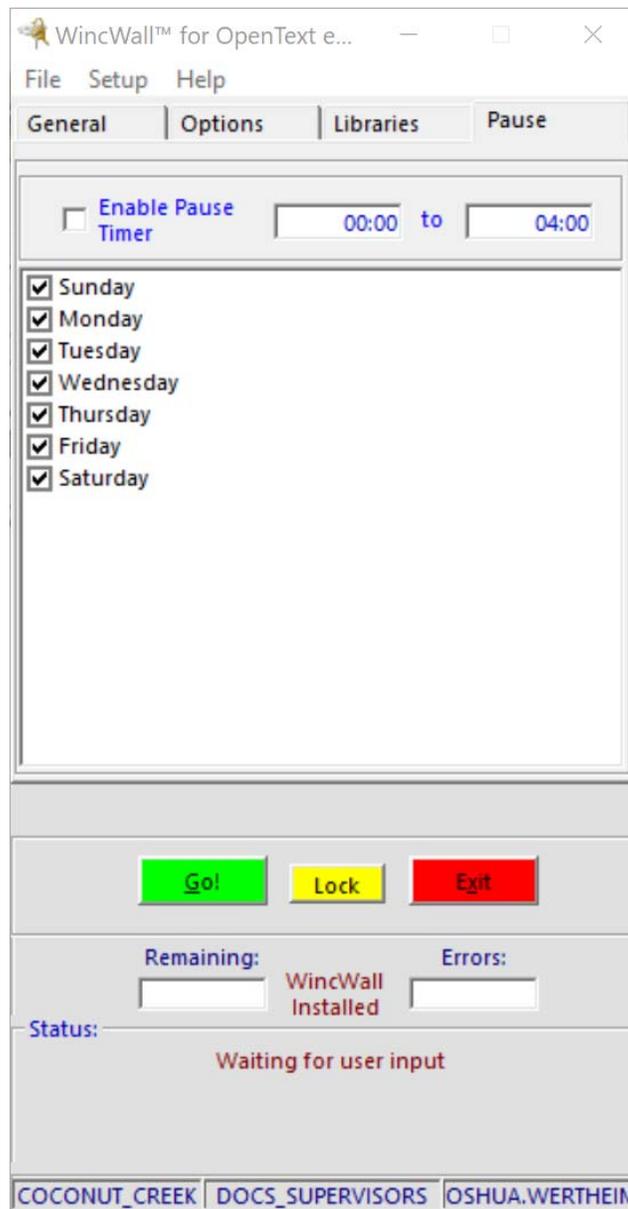
4. On the **Pause** tab, place a checkmark next to **Enable Pause Timer**, set the Start and End times in 24-hour format, and select the days you want WincWall to pause processing, i.e. for backups.

FILE MENU

View Log	F2
Purge Log	Shift+Del
Exit	Ctrl+X
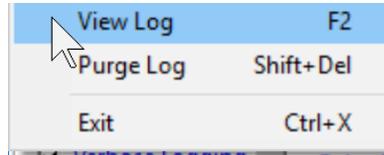
- From **File** menu you can View Log (F2), Purge Log (Shift+Del) or Exit (Ctrl+X).

SETUP MENU

Initial Setup	>
Administration	F8
Remove Duplicate Walls	
Remove Duplicate Security	
Fix Security issues	
Set Proxy Users	F11
Set Override Column	
Add Query Documents to Queue	
Add All Documents to Queue	
Add All File Parts to Queue	
Display pending documents	F7
Pending documemts by matter	
Cleanup NEEDS_SECURING	
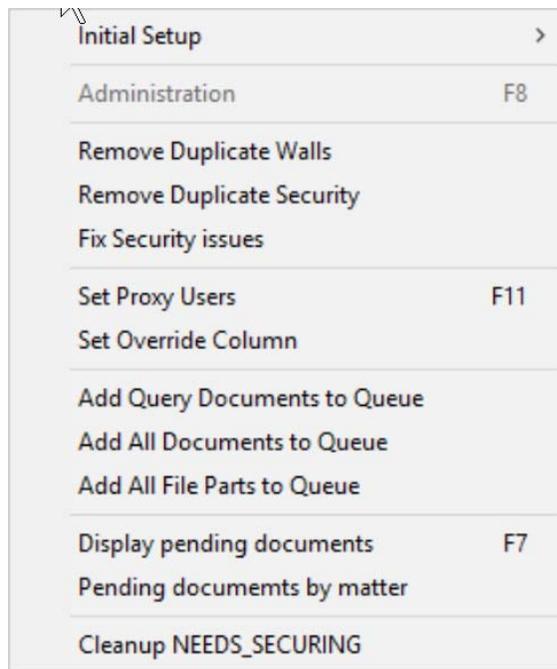
- From **Setup | Initial Setup** menu you can perform the setup options described above..

Setup a Library
Re-Install Triggers
Upgrade a library
Remove a Library
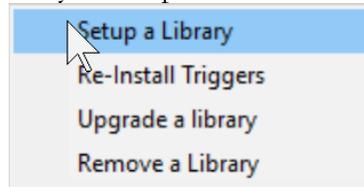
- **Administration** will launch the WincWall Admin program if it is located in the same directory as WincWall.
- **Remove Duplicate Walls** will determine if there are duplicate entries, such as the same user identified for the same wall, and clean the duplicate entries from the WINCWALL_LINK table.
- **Remove Duplicate Security** will determine if there are any profiled items that have duplicate entries in the SECURITY table, and clean the duplicate entries from the table.

- **Fix Security Issues** will review the contents of the SECURITY table, and make sure that any items that oly have users or groups with DENY rights have at least one trustee that has FULL rights. It also makes sure that there is at least one security entry for every profiled item.
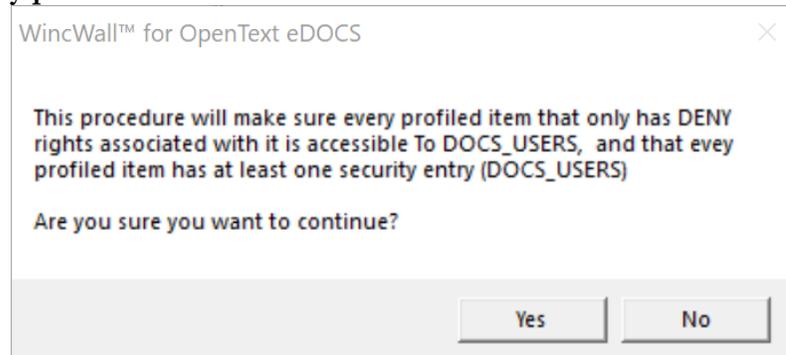
- **Set Proxy Users**: This option allows you to assign the security of a source proxy User or Group specified in a Wall to a target proxy User or Group specified by the proxy rule. You can assign a specific right template or match the security of the proxy source.
- **Set Override Column** This option will allow you to select a profile column defined in eDOCS as a checkbox column that will determine whether a document should be secured (Include) or skipped when WincWall examines the document. Typically, this would be a column on the profile form that allows the end user to decide whether to secure the document to a wall. Note that the Set to Include check box would be checked if you want WincWall to only process documents where this column is checked; conversely, uncheck this option if you want to have WincWall skip the document if the column is checked. Also note that you can select ANY checkbox column, including any you add using DM Designer.
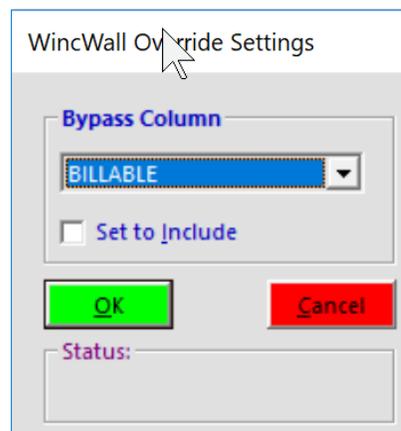
- **Add Query Documents to Queue**: Will add documents to the NEEDS_SECURING table based on a Search.
- **Add All File Parts to Queue** If you use eDOCS Records Management, and you wish to have WincWall secure file parts, you can add all the file parts into the queue using this function.
- **Add All Documents to Queue**: Will add All Documents from the Library to the NEEDS_SECURING table.
- **Display Pending Documents**: Will show the list of Documents in the Queue to be processed by WincWall, all documents in the NEEDS_SECURING table.

- **Pending Documents by Matter** Will display the number of rows in NEEDS_SECURING by their client or matter. Note that this is only available for Legal Installation.
- **Cleanup Needs Securing** Will remove rows from NEEDS_SECURING that do not match any wall. Note that this will only perform it's task if all your walls are based upon CLIENT, MATTER, or PEOPLE (author).

HELP MENU
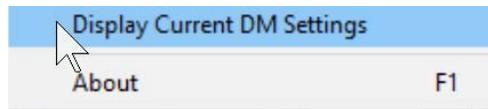
- **Display Current DM Settings**: Will display the eDOCS Library settings.
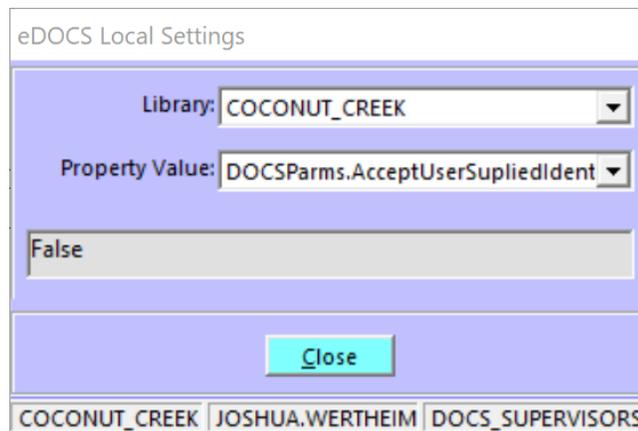
- **About**: Shows a splash screen that includes the currently installed version of WincWall, your company ID, and your serial number..

WincWall Administration

WincWall provides a separate administration module called WincWall Administration. To launch the WincWall Administration module from within WincWall, select **Administration** from the **Setup** menu and selecting the library you wish to maintain. The WincWall Administration module can also be launched by selecting **WincWall | Administration** from the appropriate library's menu in WincTools.
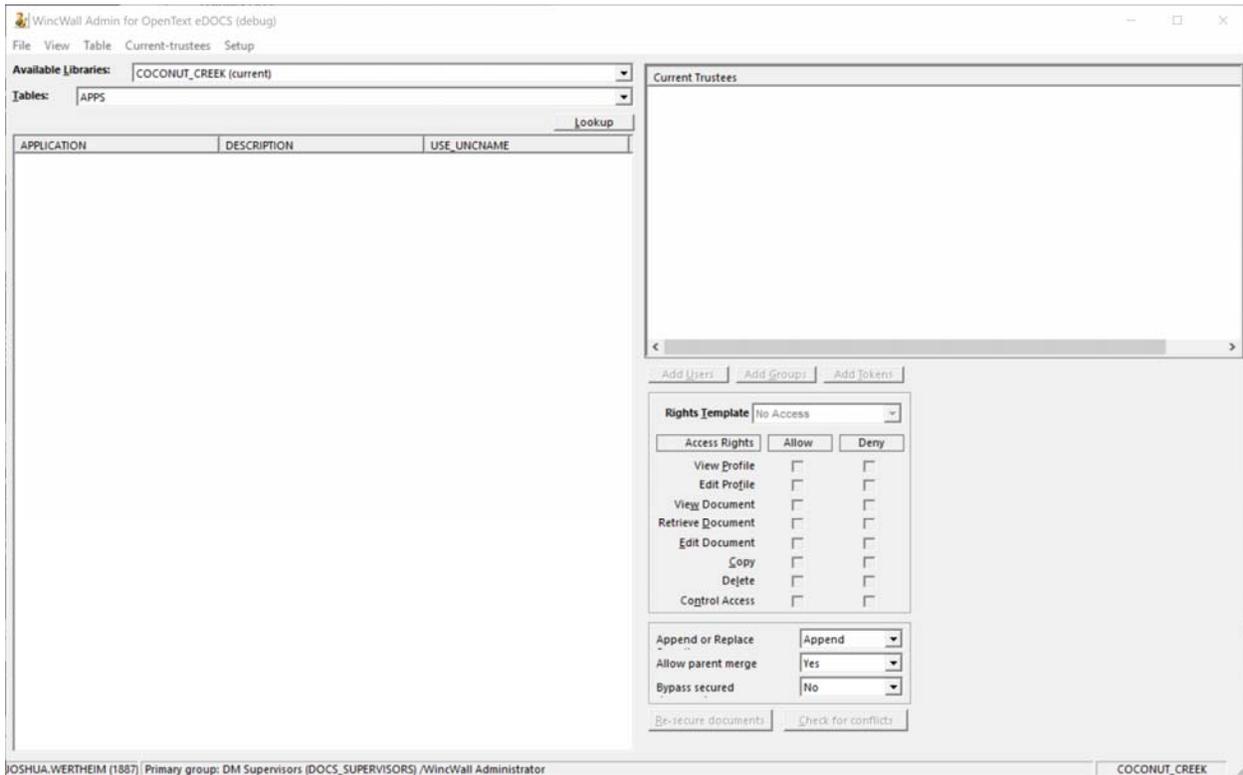
Configuring Ethical Walls

Ethical walls can be established for any item of validation data which is linked to the document profile. Some examples include Author, Client, Matter, Document Type, or Application.

To create a new ethical wall, you must first locate the value with which the wall is to be associated. There are several ways to locate validation data values within WincWall Administration:

- You can toggle between viewing only values with established relationships or all values in the table by right-clicking in the results pane and selecting either **Display All Rows** or **Filter list on existing relationships** as appropriate.
- With all rows displayed, you can search among the listed values by right-clicking in the results pane and selecting **Search**. Type in a few letters of the desired value and click OK; the first value matching the criteria entered will be highlighted.
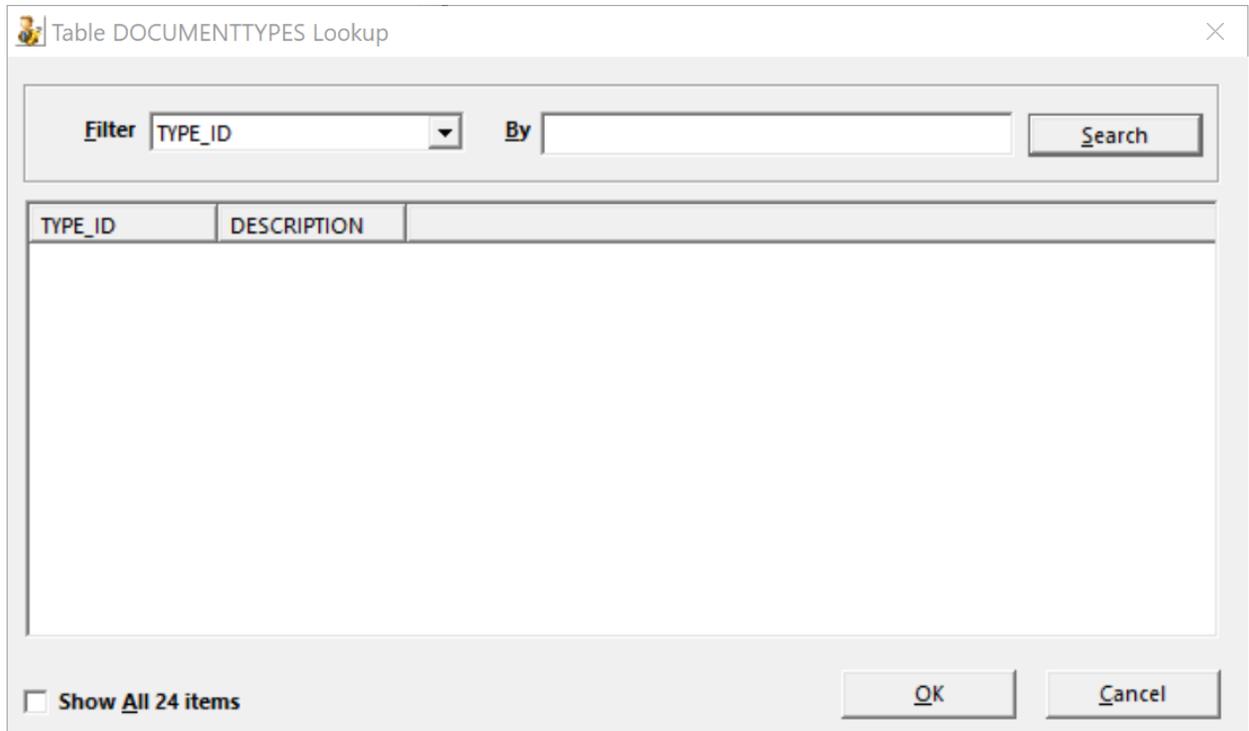
For very large tables, it may be most efficient to click on **Lookup** button under Tables list or right-click in the results pane and select **Lookup**. You will be presented with a blank lookup form for that table; you can type the first few letters of the value, or you can check the box **Show All (#) Items** to display all values in the table.

Once you have located the value around which a wall is to be built, ensure that the value is highlighted and then expand the Available Trustees to locate the users or groups to have access. Select the user(s) or group(s) and click the **Add** button to add them to the list of Current Trustees. For very long list of Users and/or Groups you can use the lookup buttons **Add Users** and **Add Groups** to manually find the required users and groups. You can also **Add Tokens** to the list of Current Trustees.

Tokens are placeholders you can use to represent runtime values specific for each document and assign security in the current wall. The available tokens for **Document Author**, **Document Typist**, **Document Author Primary Group** and **Document Typist Primary Group** will be translated to the appropriate values assign to the documents.

Add tokens   ✕

Token	Description
[Document Author]	Translates to the document's author
[Document Typist]	Translates to the document's typist
[Document Author Primary Gr...	Translates to the document author's primary gro...
[Document Typist Primary Gro...	Translates to the document typist's primary group

OK   Cancel
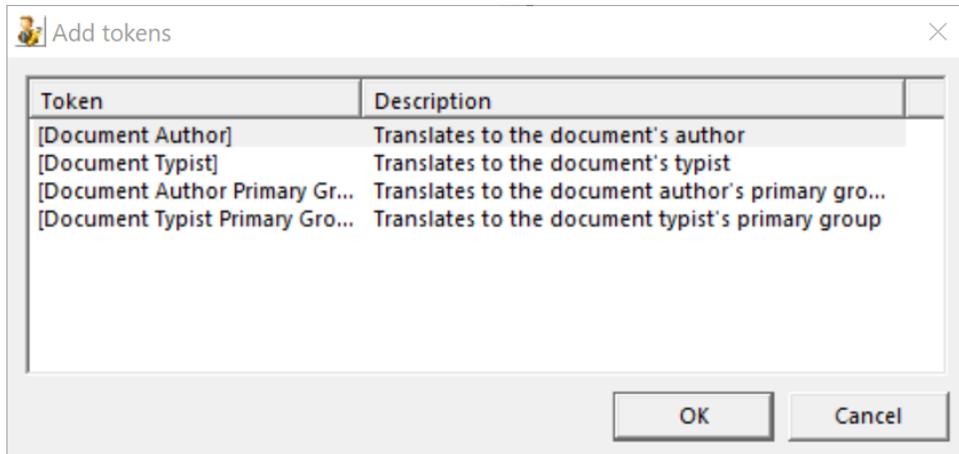
Once a user, group or token is in the Current Trustees list, you can highlight it to select the appropriate level of security to be designated. By default, trustees are added with Full Access.

Current Trustees

Corey Salm (COREY.SALM)
Developers (DEVELOPERS)
Melissa Salm (MELISSA.SALM)

Add Users   Add Groups   Add Tokens

Rights Template | No Access |

Access Rights	Allow	Deny
View Profile	☐	☐
Edit Profile	☐	☐
View Document	☐	☐
Retrieve Document	☐	☐
Edit Document	☐	☐
Copy	☐	☐
Delete	☐	☐
Control Access	☐	☐
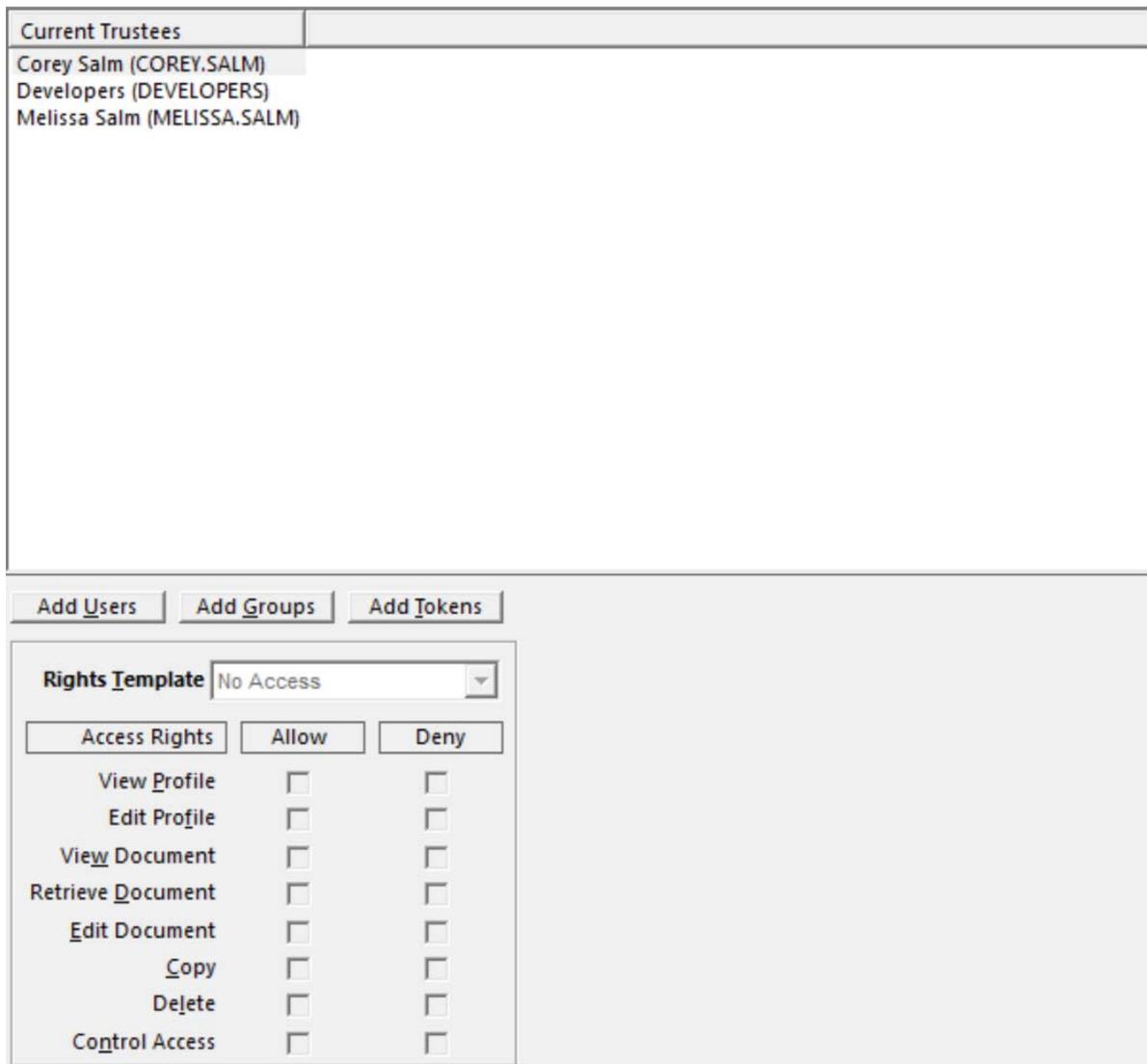
Viewing Existing Ethical Walls

The left-hand pane of WincWall Administration displays all validation data tables and, for each table, all existing ethical wall relationships. Select a table name from the drop-down list to display the values from that table for which ethical wall relationships have been established.

Click on the validation data item in the left-hand pane to view the trustees to the right.

Removing an Ethical Wall

To remove an ethical wall, right-click on the appropriate validation data item and select **Delete**. You will be asked to confirm the removal of the ethical wall. Note that this will only work if the results list is filtered to display only those rows with existing WincWall relationships.

Managing Wall Options

Append or Replace	Append
Allow parent merge	Yes
Bypass secured	No

Append or Replace Security: You can opt to use the **Default** value from WincWall general option **Append WincWall Rights to Existing Security**, specifically **Append** the security from the Wall to the existing security or completely **Replace** security with the wall security.

Allow Parent Merge If this item is the child in a Parent-Child table relationship (such as a Matter being the child of a Client), specifying Yes would tell WincWall that if the item's Parent also has a wall, merge the parent wall with this wall. Specifying No means that this wall will override any parent wall that may exist.

Bypass secured documents: You can opt to use the **Default** value from WincWall general option **Bypass documents that are already secured**, or specify whether to bypass (**Yes**) or not (**No**).

Re-secure documents	Check for conflicts

Resecure documents: Will add documents to the NEEDS_SECURING table with the criteria that match the selected wall.

Check for conflicts: Shows a Report with conflicts in access rights assigned to Groups and its members in the same wall.

```
 Report                                                                          ✕

 💾 🖨️

 ===================================================================== ⌃
Group 'LAWYERS' access rights are in conflict with its member 'CO
           ----------------------------------------------
          |            LAWYERS            |       COREY.SALM        |
           ----------------------------------------------
          |          Allow View           |                         |
          |       Allow Content View      |                         |
          |     Allow Content Retrieve    |                         |
          |       Allow Content Copy      |                         |
          |                               |        Deny View        |
          |                               |        Deny Edit        |
          |                               |    Deny Content View    |
          |                               |  Deny Content Retrieve  |
          |                               |    Deny Content Edit    |
          |                               |    Deny Content Copy    |
          |                               |   Deny Content Delete   |
          |                               |   Deny Access Control   |
           ----------------------------------------------
                                                                     ⌄
 ◁ ▭▭▭▭▭▭▭▭▭▭▭▭▭▭▭▭▭▭▭▭▭                                        ▷
```
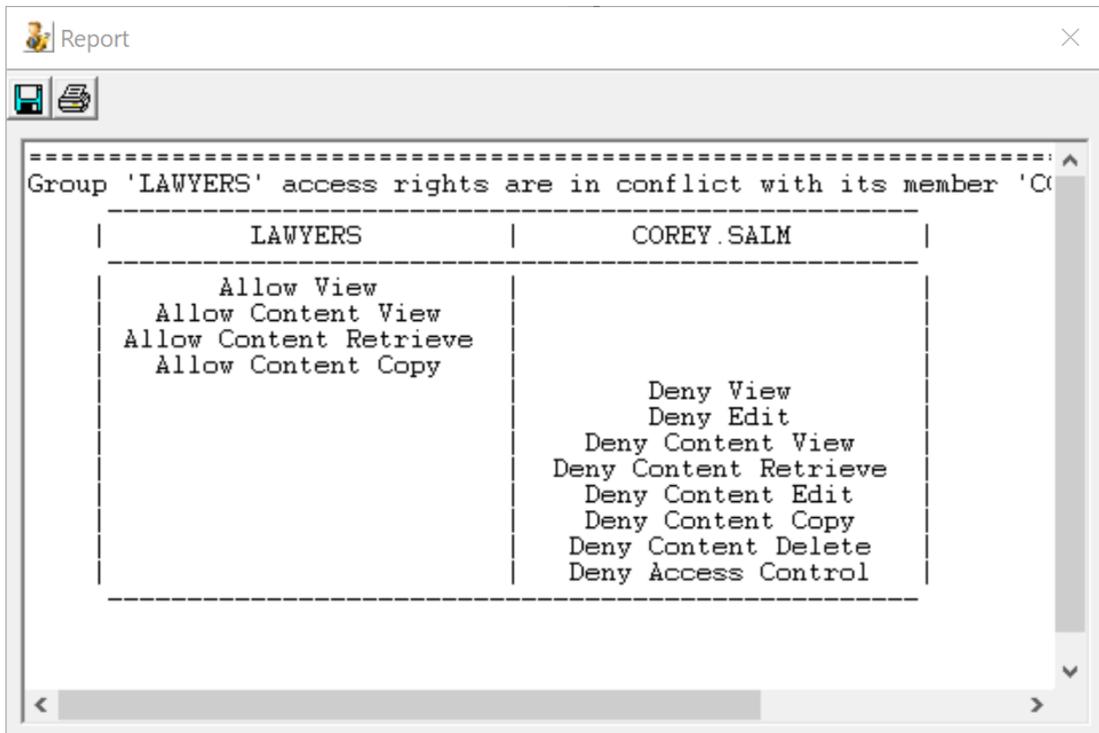
Using WincWall with WincTools
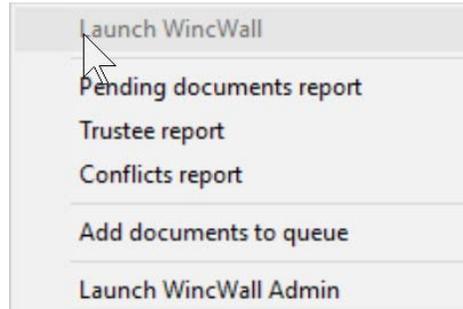
As previously stated, from WincTools, by right-clicking the Library where WincWall is installed you can go to the WincWall sub-menu to execute some functions of WincWall. The following actions can be performed from within WincTools:

Launch WincWall: Run the stand-alone version of WincWall.

Pending documents report: Will show the list of Documents in the Queue to be processed by WincWall; all documents in the NEEDS_SECURING table.

*Trustee report: This report will generate a list of all Walls currently in use by WincWall by displaying the trustee (users or groups) used by the walls.

*Conflicts report: This report will generate a list of all conflicts in access rights assigned to Groups and its members in the same wall for all walls in use.

Add documents to queue: Will add documents to the NEEDS_SECURING table based on a Search.

Launch WincWall Administration: Run the stand-alone of WincWall Administration module.

* These features are only available from WincTools.

Security Classification Support

With versions of WincWall dated April 15, 2010 and later, security classifications are supported in eDOCS 5.x as close to the way it works with eDOCS 6.x as possible. This support will assign security to each individual document based upon the clearance-level set on the document, and adds each group or people trustee to the security of the document based upon that user or group's clearance level.

In order to use security classifications with WincWall, some customizations to the eDOCS 5.x database must be performed; specifically, the addition of a table called CLASSIFICATION, the addition of a profile link to the CLASSIFICATION table, and the addition of links in the PEOPLE and GROUPS table to the CLASSIFICATION table. All of these customizations can be performed using the DM Designer tool, using the 'super user' command-line switch (**paint32.exe /xyzzy**). This section describes the general steps required in order to complete the customization required, and assumes that the user has a familiarity with using DM Designer.

1. Create the CLASSIFICATION table

    a. Add two columns to the table

        i. DESCRIPTION – Candidate Key, String, 48 characters

        ii. CLASSIFICATION – Integer

    b. Create a lookup to the CLASSIFICATION table

    c. Create a unique index on the CLASSIFICATION table on the DESCRIPTION and CLASSIFICATION columns.

    d. When you save the table, make sure to create a link from the PROFILE table to the CLASSIFICATION table. The column in the PROFILE table will be called CLASSIFICATION.

    e. Create a maintenance form for the CLASSIFICATION table for entry of the CLASSIFICATION and DESCRIPTION information for each classification level.

2. Add the CLEARANCE column to the PEOPLE and the GROUPS tables, as Foreign keys to the CLASSIFICATION table.

    Note that WincWall Admin is enhanced to add a function called 'Set Security Clearances', and this method of maintaining user and group clearances will be the recommended method, since it will automatically add documents into the WincWall queue for processing additions/changes to document security.

3. Add the CLASSIFICATION column (the foreign link, not the actual profile column) to your profile entry and search forms.

4. Save your changes and exit DM Designer.

5. Add at least one entry into the CLASSIFICATION table, with the CLASSIFICATION of zero (0) and the DESCRIPTION of 'Unclassified'.

6. Optionally run the following three SQL statements:

    UPDATE DOCSADM.PROFILE SET CLASSIFICATION = (SELECT SYSTEM_ID FROM DOCSADM.CLASSIFICATION WHERE CLASSIFICATION = 0)

UPDATE DOCSADM.PEOPLE SET CLEARANCE = (SELECT SYSTEM_ID FROM DOCSADM.CLASSIFICATION WHERE CLASSIFICATION = 0)

UPDATE DOCSADM.GROUPS SET CLEARANCE = (SELECT SYSTEM_ID FROM DOCSADM.CLASSIFICATION WHERE CLASSIFICATION = 0)

WincWall will then examine each document to see if it's CLASSIFICATION is non-zero. If it is non-zero, it gathers the list of all users and groups that have a CLEARANCE that is equal to or greater than the document's classification, and adds those users and groups into the security of the document.

Groups get assigned rights based upon the group's UNIV_ACCESS setting, DOCS_USERS who, if specified, get view profile rights; and DOCS_SUPERVISORS who, if specified, get full access.

People get assigned access rights of 63 (all rights except DELETE and CONTROL ACCESS), except the author and/or typist who, if specified, get all rights.

Note that classification security overrides WincWall security. If a document was to be walled by WincWall, but the document is assigned a classification, the classification is processed and not the wall.

Setting Security Classifications

To set security classifications for users and groups, go to the WincWall setup menu and select the option **Set Security Clearances**. A screen similar to the following will appear:

To change the clearance for a user or a group, select the item by clicking and HOLDING the mouse button on the value to change, until a drop-down list appears, such as:

Select the value you wish to assign to the user or group, and then press the Tab key or select another user or group.

To save your changes, press the **Save** button, to cancel saving your changes, press the **Cancel** button.

Notes:

1. The user running WincWall or WincWall Admin can only change clearances for users or groups that have a clearance LOWER than or EQUAL to their own clearance;

2. The user running WincWall or WincWall Admin can only set a clearance that is LOWER than or EQUAL to their own clearance.

3. When the changes are saved, WincWall or WincWall Admin will immediately add the users and groups to the security values of all items in the library that their clearance allows. The documents are not added to the WincWall NEEDS_SECURING table.

The WincWall_Link table

The WincWall_Link table is used to store all of the information related to a wall. Each item secured by WincWall (client, matter, doctype, etc.) will have one or more entries in the table that define the wall and how WincWall will secure the documents inside that wall.

For each wall, there are four pieces of information that are retained in the table. These are stored in the TABLE_NAME, THING, PERSONORGROUP and ACCESSRIGHTS columns.

Basic WincWall information for users and groups

The TABLE_NAME column identifies the table in which the walled item exists. Note that the table name is preceded by the text '[OWNER].', which gets replaced with the actual owner of the table (in most instances, DOCSADM). The variable [OWNER] is placed in the column because there may be different database owners in a multi-library environment, particularly with Oracle or MS SQL 2008.

The THING column identifies the SYSTEM_ID of the walled item in the table identified by TABLE_NAME. As an example, the THING of 12345 in the table [OWNER].MATTER refers to the matter in the table that is assigned the SYSTEM_ID of 12345.

The PERSONORGROUP column identifies the user or group who should then be assigned the ACCESSRIGHTS specified.

To put this all together, a row may have the following information:

TABLE_NAME	[OWNER].MATTER
SID	12345
PERSONORGROUP	98765
ACCESSRIGHTS	0

WincWall will then assign the accessrights of 0 (which gets translated as 'DENY') to the user or group with the SYSTEM_ID of 98765 to all of the documents that are in the PROFILE table with a MATTER that has a system_id of 12345.

If there are multiple users or groups to have security assigned to the same matter, each one will have its own row in the WINCWALL_LINK table.

Please note that there are additional columns in the WINCWALL_LINK table that are not used and are therefore not described herein.

Additional Option information stored in WINCWALL_LINK

There are three additional rows that are added into the table for each wall that define the options related to how WincWall will process the documents in the wall. These three options have a value set in the PERSONORGROUP column in WINCWALL_LINK:

- Append or overwrite security of documents in the wall (-1)

- Use Typist/Author overrides that are set in the WincWall program (-3)

- Whether to Bypass Secured documents (-5)

For each of each of the above three options, there are three choices to make, each of is set in the ACCESSRIGHTS column in WINCWALL_LINK:

- Default (0) [Note that Default refers to the default option as it is set in the WincWall program itself and it is not recommended that you use this setting.]

- No (-1)

- Yes (1).

As an example, let's say that for the wall that is defined for the MATTER with THING (system_id) 12345, we wish to overwrite security, to allow WincWall to assign the Typist/Author Overrides, and not to Bypass Secured Document.

The entries in the WINCWALL_LINK table for these three options would therefore be:

COLUMN	VALUE	EXPLANATION
TABLE_NAME	[OWNER].MATTER	
THING	12345	The system_id of the item for which the rule is established
PERSONORGROUP	-1	Minus 1 (-1) refers to the option to Append or Replace Security
ACCESSRIGHTS	1	1 Means Yes

COLUMN	VALUE	EXPLANATION
TABLE_NAME	[OWNER].MATTER	
THING	12345	The system_id of the item for which the rule is established
PERSONORGROUP	-3	Minus 3 (-3) refers to the option to use the WincWall

		Typist/Author Overrides
ACCESSRIGHTS	0	0 means Default

COLUMN	VALUE	EXPLANATION
TABLE_NAME	[OWNER].MATTER	
THING	12345	The system_id of the item for which the rule is established
PERSONORGROUP	-5	Minus 5 (-5) refers to the option to Bypass Secured Documents
ACCESSRIGHTS	-1	-1 means No

Additional Token information stored in WINCWALL_LINK

There are then up to four additional rows that are added into the WINCWALL_LINK table for each wall, that are used when Tokens (variables) are defined that get replaced with the actual values for each document.

Four Tokens are available for each wall: the document's Typist (-4), its Author (-2), the typist's Primary Group (-16) and author's Primary Group (-8).

When WincWall processes a document in the wall, if a token is assigned to the wall, the program replaces the token with the actual user or group, and then assigns that user or group the security defined in the ACCESSRIGHTS column associated with the token.

As an example, let's say that for the wall that is defined for the MATTER with THING (system_id) 12345, we wish to set security for the document's author to Normal rights, the typist's primary group to read-only, and the author's primary group to deny. The entries in the WINCWALL_LINK table for these options would therefore be:

COLUMN	VALUE	EXPLANATION
TABLE_NAME	[OWNER].MATTER	
THING	12345	
PERSONORGROUP	-2	Minus 2 (-2) refers to the token for each document's Author
ACCESSRIGHTS	63	Normal rights

COLUMN	VALUE	EXPLANATION
TABLE_NAME	[OWNER].MATTER	
THING	12345	
PERSONORGROUP	-16	Minus 16 (-16) refers to the token for each document's typist's Primary Group
ACCESSRIGHTS	45	Read-only

COLUMN	VALUE	EXPLANATION
TABLE_NAME	[OWNER].MATTER	
THING	12345	

PERSONORGROUP	-8	Minus 8 (-8) refers to the token for each document's author's Primary Group
ACCESSRIGHTS	0	Deny

Security scenarios based upon rule setup

Different scenarios in a rule will produce different results. The following explains in detail the results that you should see, based upon how rules are established.

Scenario 1:

All the trustees in WincWall are Denied rights. DOCS_USERS is not included in the trustee list.

Result: The trustees will be added to each document with DENY rights, and DOCS_USERS will be added with full rights. The assumption is that only those being denied access should have the document(s) hidden and everyone else should have access to the document(s).

Scenario 2:

All the trustees in WincWall are Denied rights. DOCS_USERS IS included in the trustee list.

Result: The trustees will be added to each document with DENY rights, and DOCS_USERS will be added with the explicit rights stated in the rule.

Scenario 3:

At least one trustee in WincWall is granted at least some rights. DOCS_USERS IS NOT included in the trustee list.

Result: The trustees will be added to each document with the rights explicitly granted or denied them. DOCS_USERS will NOT added. The assumption is that DOCS_USERS should not be granted any rights to the document(s).

Scenario 4:

At least one trustee in WincWall are granted at least some rights. DOCS_USERS IS included in the trustee list.

Result: The trustees will be added to each document with the rights explicitly granted or denied them. DOCS_USERS will be added with the explicit rights stated in the rule.

NOTE:

Unless author and typist rights are overridden using the tokens, AUTHOR and TYPIST will always be added, and granted full rights.

If the author and/or typist rights are overridden using the tokens, the rights defined for them by the token will be added to the document.

However, if a rule is setup where there are no users or groups that have full rights to the document, WINCWALL will automatically ensure that the TYPIST gets full rights, regardless of the rights granted the typist by the token setting, so that there is at least one person or group with full rights to every document.