WincWall Security Settings Chart

(Applies to versions dated September 9, 2018 and later)

	All wall trustees denied rights (Exclusionary Wall)		Not all wall trustees denied rights (Inclusionary Wall)	
	Append	**Replace**	**Append**	**Replace**
Unsecured items	1. Add wall trustees 2. Add DOCS_USERS with full rights 3. Add Author/Typist with full rights	1. Add wall trustees 2. Add DOCS_USERS with full rights 3. Add Author/Typist with full rights	1. Add wall trustees 2. Remove DOCS_USERS unless part of the wall 3. Add Author/Typist with full rights	1. Add wall trustees 2. Remove DOCS_USERS unless part of the wall 3. Add Author/Typist with full rights
Secured items	1. Add wall trustees	1. Remove existing security 2. Add wall trustees 3. Add DOCS_USERS with full rights 4. Add Author/Typist with full rights	1. Add wall trustees	1. Remove existing security 2. Add wall trustees 3. Add Author/Typist with full rights

What WincWall does when a wall is removed	
Option:	**Description:**
Remove all security	Remove all trustees, add DOCS_USERS with full rights, unsecure document
Remove deny rights	Remove all denied trustees; if only DOCS_USERS remain, unsecure document
Secure to Author & Typist only	Remove all trustees, add AUTHOR and TYPIST with full rights

Notes:

1. An Inclusionary wall is a wall with any combination of rights, where at least ONE of the trustees in the wall is not denied rights; an Exclusionary wall is a wall where all listed trustees are denied access.
2. When DOCS_USERS is included as a trustee with full rights, and all other trustees are denied access, the wall will still be considered Exclusionary.
3. Where specified above, DOCS_USERS are only added to an Exclusionary wall if there are no other trustees (besides author and typist) that are added with full rights.
4. If a wall includes a token for Author or Typist, with rights other than full, the token rights will supersede the user's rights unless the author's or typist's ID is explicitly listed as a trustee in the wall.
5. When WincWall secures an item, it links the PROFILE SECURITY_LINK column to the PROFILE's SYSTEM_ID, and sets it's SEC_REASON_LINK to 99 (WincWall), which is added to the SEC_REASON table.
6. When WincWall un-secures an item, it sets the PROFILE's SECURITY_LINK and SEC_REASON_LINK values to zero.
7. Detail of individual additions, changes and deletions are recorded in the WINC_AUDIT_SEC table
8. Before and after snapshots of security changes are recorded in the WINC_SECURITY table. Before snapshots are identified with a negative ACCESSRIGHTS value.
9. The most recent change (per day) made by WincWall is recorded in the ACTIVITYLOG table, to avoid clutter when a document is secured multiple times during that day.

File Part Security Mapping

Commencing with versions of WincWall dated September 9, 2018, Records and File Parts are secured if they are identified as part of a wall.

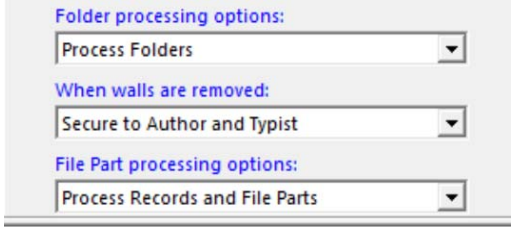
WincWall identifies whether a File Part is in a wall by determining whether or not there is a column in the PD_FILE_PARTS table that is linked to the MATTER table, and if there is, and the linked matter is in a wall, then that matter's trustees are assigned rights that correspond to each trustee's designated rights.

Because there are differences between document rights and file part rights, WincWall must map the wall rights to corresponding file part rights. The below chart describes how this mapping works.

Profile Rights	File Part Rights	File Part Security Value	Mapped Wall AccessRights
View	View Term	1	1 to 5 except 3 (normal)
	View File Part		
Read-Only	View Term	257	4, 6, 8, 9, 10, 12, 13
	View File Part		
	Assign to File Part		
Normal	View Term	259	3, 7, 11, 14 to 63
	View File Part		
	Assign to file part		
	Edit file part		
	Create File		
	Change File Name		
	Cut and Paste File		
Near-Full Access	All but Delete File Part and Control Access	323	64 to 127
Full Access	Normal, plus	451	127 to 255
	Delete File Part		
	Control Access		
	Create Narrower Term		

The RECORDS_MANAGERS group is always added to the security of a file part, with accessrights of 511; and when DOCS_USERS are identified, they get accessrights of 301.

To enable securing file parts, go to the Options tab in WincWall and set the File Part processing option to "Process Records and File Parts":



WORKSPACE SECURITY

Commencing with versions of WincWall dated March 22, 2019, WincWall will secured shared Workspaces on systems with eDOCS version 16.x or later.

In order for WincWall to support this feature, the WORKSPACE_FORM will need to be modified using DM Designer to add the profile columns related to any column that is the basis for a wall. For instance, if you have Matter walls, you will need to add the PROFILE.MATTER.CLIENT_ID.CLIENT_ID and PROFILE.MATTER.MATTER_ID columns to the form.

Then, when a Workspace is created or edited, if the user sets the form's value to an item in a wall, WincWall will share it to any user or group that is allowed to see other items (documents, emails, folders, etc.) for that walled item. Note that unless DOCS_USERS is explicitly identified in a wall with some allow rights, DOCS_USERS will not be added to the Workspace security.

WincWall sets the workspace security as follows:

- All rights in the Wall maps to all rights for the Workspace
- All rights except Control Access maps to all rights except Control Access for the Workspace
- Any other allowed rights maps to normal rights to the Workspace.