



Avoiding Common Security Pitfalls in ProjectWise

Kevin van Haaren, HNTB

Mid-America CADD Community
2013 Conference



HNTB's Security Philosophy

- Paranoia without insanity
- Minimize chance for making mistakes
 - Many eyes review
 - Minimize changes over life of project
- Centralized control
- Per Project Role-based Security
 - Works well for consulting engineers
- Laws
 - Subfolders more than 2 below project root must inherit
 - No per document security
 - User Access Lists applied to folders/files. No individual users or groups.



ProjectWise Security

- User Settings + File/Folder Security + Workflow Security
- Brand new datasource
 - Default is no File/Folder Security applied
 - Everyone has read/write/modify files & folders
 - Administrators can change permissions
 - Owners of folders can change permissions



Datasource Security

- HNTB settings:
 - Folder
 - Administrator Group: Create/Delete/Read/Write
 - *Everyone: Read
 - Files
 - Administrator Group: Create/Delete/Read/Write
 - Datasource Settings > Miscellaneous > Grant implicit 'Change Permissions' to owner of projects, folders, & documents
 - OFF! OFF! OFF! OFF! OFF!



Datasource Security

KvHDev (Admin) Properties

General | Security | Database Users | Spatial | Revit Integration
Managed Workspace | Settings | Icons | Statistics | Audit Trail
Folder Security | Document Security | Granular Security

Inherited from: none (item own permissions)

Name	Domain
Administrator	
Everyone	

Add...
Remove

Permissions:

- Full control
- Change permissions
- Create
- Delete
- Read
- Write
- No access

OK Cancel Apply

KvHDev (Admin) Properties

General | Security | Database Users | Spatial | Revit Integration
Managed Workspace | Settings | Icons | Statistics | Audit Trail
Folder Security | Document Security | Granular Security

Inherited from: none (item own permissions)

Name	Domain
Administrator	

Add...
Remove

Permissions:

- Full control
- Change permissions
- Create
- Delete
- Read
- Write
- Change Workflow State
- File Read
- File Write
- Free
- No access

OK Cancel Apply



User Settings

- General
 - Use access control
- Administrative
 - Display Access Control
- Document
 - Create/modify/delete/free
 - Set/Remove Final Status
- Folder
 - Create/modify/delete
- Project Permissions
 - Allow user to change Project Types and Project Properties:
can create global saved searches in a project



General Tips and Issues

- Turn off Access Control setting for full administrators
 - Indexing, Composition/Automation account, not user sync
- Use the Access Control pane
 - Unless you want to list a group with folder permissions but not file permissions
- User in multiple groups/access lists
 - Most permissive permissions are used
 - If you are in a group that allows something: you can do it
 - EXCEPT:
 - No Access ALWAYS applies!
- Everyone
 - Means everyone with Use Access Control on
 - Everyone No Access will block everyone!



User Access Control lists for security

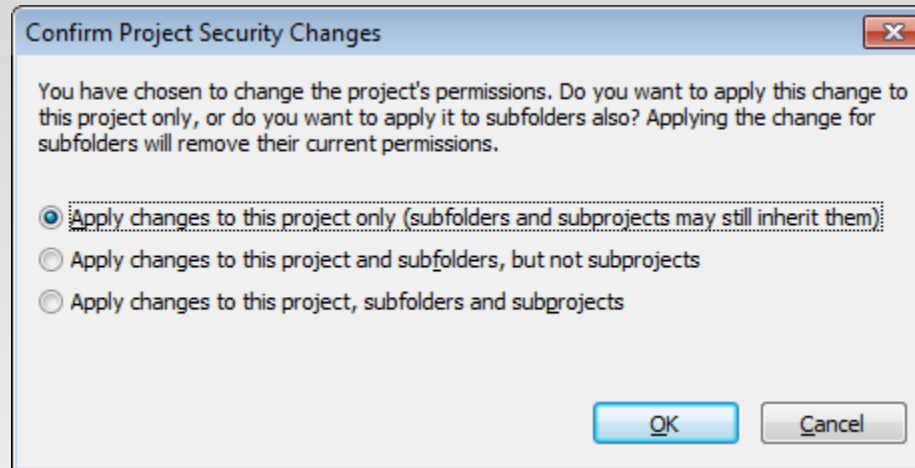
- User Access Lists can contain Users, Groups, other User Access Lists
- Removing a group's permissions: remove from the appropriate user list
 - Member Of tab
- Removing a user's permissions: remove from group or user list
- “Give Group Z the same permissions as Group X”
- Day 1: “Remove Company B's access!”, Day 20: “Restore Company B's access exactly as before!”



File & Folder Permissions Are Separate

- Not having access to a folder DOES NOT mean you don't have access to the files.
- No Access Folder, Access Files
 - Files can be found via search
- No Access Root Folder, Access Lower Folder
 - Can create custom folder shortcut to lower folder
 - Folder can be found via search (Search Builder)

Applying Permissions



- First option is safest. Only changes current folder. Any folder below that inherits will inherit these permissions
- Changes current folder. Any subfolder has permissions removed, set to inherit. Subprojects not changed.
- All subfolders and subprojects will have existing security removed and set to inherit. THERE IS NO UNDO.



Security Report + Import/Export

- Access Control > Excel icons on far right of toolbar
- Export to generate report listing all permissions
 - Save for “undo” of permissions changes
 - Search for particular groups/users used in deep security
 - Store with archive so security can be recovered
- Import to set permissions per spreadsheet
 - Merge vs. Replace