



### Comprehensive, flexible control of information.

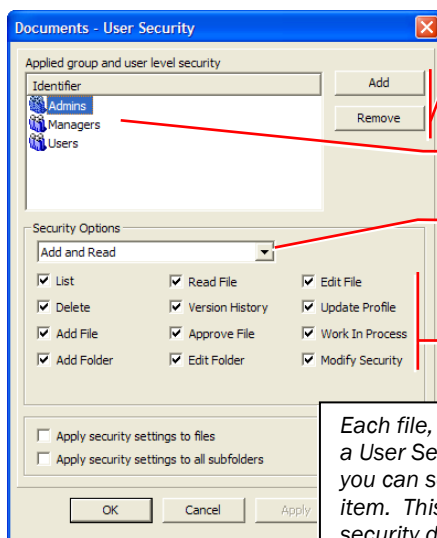
Document Locator provides a comprehensive set of security and auditing capabilities based on the familiar Microsoft® NT security model. You maintain your own data with complete flexibility to manage authentication credentials, and to grant access and activity privileges on a user or group basis. This means you control not only who accesses the information but how the information is accessed and what can be done with it.

### Control access with user accounts and security groups.

Creating user accounts is easy because Document Locator can selectively import your Windows user list, and from there, you can assign users to one of three default security groups—Administrator, Manager, or User—or, you can define your own group. Document Locator is also integrated with Microsoft Active Directory, which means that as new users are added to the system through Active Directory, the system administrator can add them to security groups.

### Control access to directories, folders, and documents.

Once you've created user accounts, you can then grant access to documents on a group or individual user basis. You select the security level or the options you want a user or group to have for the selected directory, folder, or file. You can set a folder's security and then apply the settings to sub-folders and documents within them, or you can hide restricted folders from view entirely.



Use the buttons to add / remove users and groups to / from this document's security.

Assign users to one of three pre-defined groups, or define your own group.

Select a security level from the Security Options list to add or remove access rights for the selected user or group.

Or, customize security by selecting individual activity options here.

Each file, folder, and directory has a User Security dialog box where you can set up security for that item. This example shows the security dialog box for the Documents directory.

### Benefits

- **Information control** – Controls access down to the file and feature level. Comprehensive, flexible security tools provide control over virtually every aspect of the repository and system, giving you truly secure information.
- **Audit trail** – Logs custom-specified user activity and user attempts.
- **Integrated with Microsoft Active Directory** – Manage system access using Active Directory.
- **Encryption options** – Safeguards information by supporting encryption for business processes involving sensitive information.

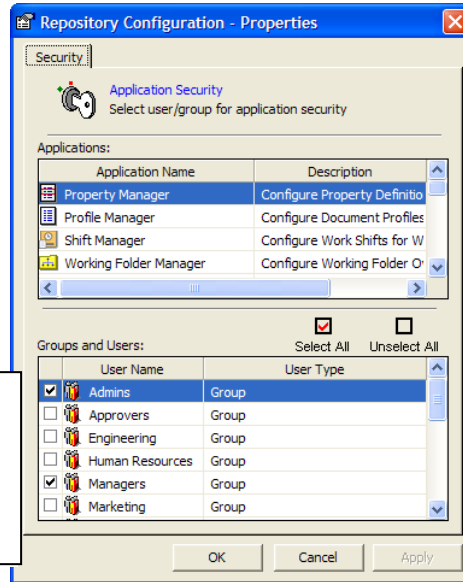
### Solutions

- **Security and business continuity** – Control view and access rights to files, folders, directories, and repository tools.
- **Regulatory compliance** – Prevent users from seeing restricted folders containing sensitive information such as HR documents or medical records.

## Control access to repository configuration tools.

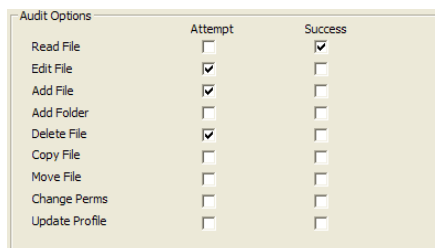
Manage access to administrative tasks and repository configuration tools by controlling which tools users and groups can access. For example, to prevent uncontrolled and inconsistent metadata creation, you can restrict access to the Property Manager and Profile Manager. Users will not even see the tools to which they do not have access.

*This example shows that only members of the Admins and Managers groups have access to the Property Manager.*



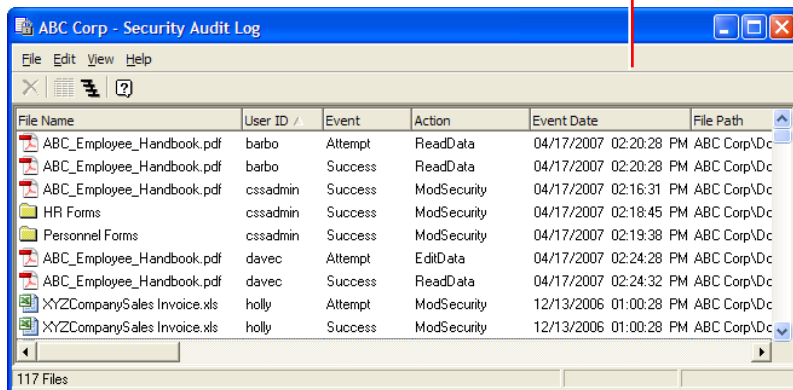
## Monitor user activity on specified documents and folders.

The auditing feature enables you to track certain types of user activity performed on specified folders and files. When you set up auditing on a folder or file, a record of the tracked activities is recorded in the Security Audit log. You can configure auditing to track activity attempts, successes, or both. The log shows who performed what activity on which files and folders, and when. Administrators can restrict access to the Security Audit Log.



*Each setting controls whether an entry appears in the audit log.*

*When these options are enabled, the corresponding file activities are registered in the Security Audit log file.*



## Related Features

- **Automated Workflow** – Protect automated business processes from unauthorized use.\*
- **Check-out and Check-in** – Configure security to prevent users from checking out restricted documents.
- **Document Approval** – Protect the approval process by requiring approvers to supply a password.
- **Email Management** – Protect imported email from unauthorized access.\*
- **Folder Properties** – Automatically apply security settings to documents on import.
- **Notification Subscriptions** – Receive a notification when restricted files or folders are accessed.
- **Records Management** – Ensure compliance with government and industry regulations.
- **Searching** – Create and protect custom searches.
- **Version Control** – Restrict access to earlier document versions.
- **Web Access** – Enable secure remote access to repositories via the Web.\*

For more information about products or purchasing, please visit:

[www.documentlocator.com](http://www.documentlocator.com)

**ColumbiaSoft Corporation**  
10300 SW Greenburg Rd.  
Suite 180  
Portland, OR 97223  
(503) 274-0504  
(800) 298-1172

\*Optional module required.