FileDirector®
Document Management System

Security

No Rights, No Access

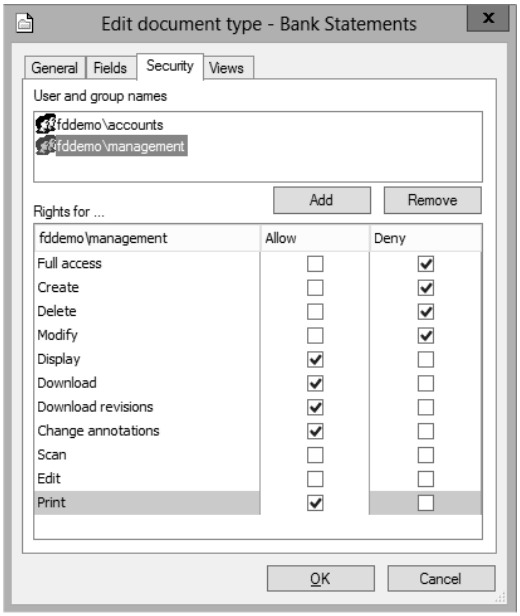
FileDirector is a highly secure document management solution that ensures that documents are only accessible to those user accounts that have been granted permission to them.

Keep your documents safe and secure

Active Directory

FileDirector utilises Active Directory users and groups for access control. No account can gain access to FileDirector without being a member of one of the FileDirector Groups. When a user account is a member of one of the FileDirector groups, this does not by default give them access to any of the data stored in FileDirector.

Where the preference is not to incorporate Active Directory, FileDirector also has its own proprietary security that works in exactly the same manner but is configured within FileDirector.



No Direct Access to Data

FileDirector is a client server solution, with ALL requests from clients for data being serviced by the server application. User accounts do not require permissions to either SQL or the locations where documents are stored.

Communication Encryption

The FileDirector Server is an IIS web service and can therefore take advantage of IIS encryption features, to secure the data being sent to and received from a client. IIS can secure communication using up to a 128bit key, Alternatively, certificates can be implemented to further secure the communication.

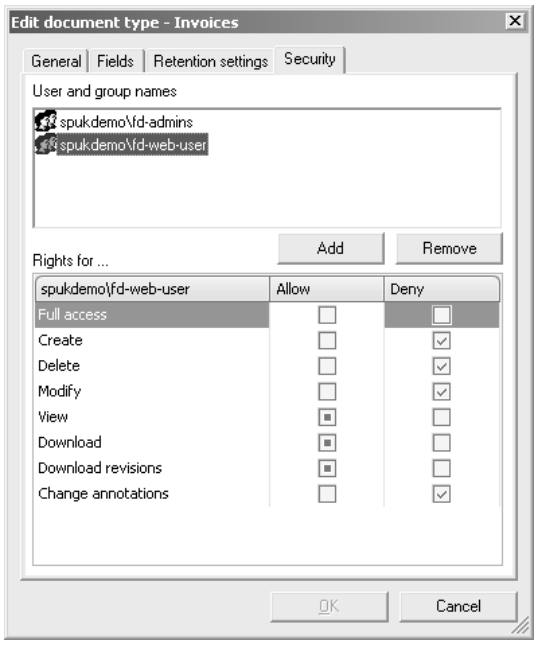
Document Management made easy...

FileDirector®
Document Management System

Cabinet Security

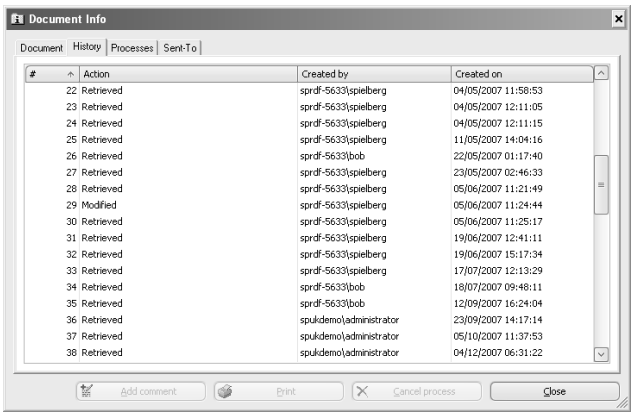
Document management applications are created in FileDirector Cabinets. When a user account is valid for FileDirector, unless the account or user group has been granted access to a Cabinet, the account will have no access to a cabinet. Additionally, Cabinets can be designed so that different Document Types and/or storage applications are created in a single cabinet. A user account or group can be assigned or denied access to each Document Type/application within a Cabinet. Different levels of access can be assigned to an account or group for each Document Type/application they have access to. As an example, in one a user may be able to create documents, but in a second application that same account may only be able to retrieve and view documents.

A further level of security can be applied to secure documents, and this is done at application field level. Access to documents can be determined by the value held within fields, either allowing or denying access to accounts or groups.



Auditing

All activity within the FileDirector solution can be logged, and stored for future reporting. For each document, a history is kept that details the activities associated with the document. This history will list, for example, the accounts that have created, modified and retrieved the document. It will also show when those activities took place.



Microsoft® CERTIFIED Partner

Spielberg

www.spielbergsolutions.com