Spielberg Solutions GmbH

FileDirector

Enterprise & SBE

Installation Guide

Version 3.0

Disclaimer

Spielberg Solutions GmbH makes no representation or warranties with respect to the contents or use of this document and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Spielberg Solutions GmbH reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Spielberg Solutions GmbH makes no representations or warranties with respect to any FileDirector software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Spielberg Solutions GmbH reserves the right to make changes to any or all parts of FileDirector software, at any time, without obligation to notify any person or entity of such changes.

Africa, Asia, Australia, Europe and USA

Spielberg Solutions GmbH
Obere Kaiserswerther Str. 17
D-47249 Duisburg
Germany
Email: *info@spielberg.de*
Web: *www.spielberg.de*

UK and Eire

Spielberg Solutions Ltd
Unit 11
Basepoint Business Centre
Metcalf Way, Crawley
RH11 7XX, UK
Email: *info@spielbergsolutions.com*
Web: *www.spielbergsolutions.co.uk*

Software Licence Agreement

IMPORTANT: Read this agreement before installing FileDirector. By installing FileDirector you are deemed to agree to be bound by this agreement.

This license agreement is a legal document between you and Spielberg Solutions GmbH. If you do not agree to the terms of this agreement return the software CD and accompanying documentation (the "Documentation") and other items to the place from where you obtained them for a refund before they are marked or damaged in any way.

In consideration of the right to use the Software you agree to abide by the terms and conditions of this agreement.

GRANT OF LICENSE

The Software consists of the software modules by:

Spielberg Solutions GmbH, a German public listed company having its place of business at Obere Kaiserswerther Str. 17, 47249 Duisburg, Germany ("Spielberg");

Microsoft Corp., a Washington Corporation having its place of business at 1 Microsoft Way, Redmond, WA 98052-6399, USA ("Microsoft");

MICROPLEX Trading GmbH, a German Company having its place of business at Leipziger Chaussee 191g, 06112 Halle, Germany("Microplex");

Nuance Communications International BVBA., a Belgian Company having its place of business Guldensporenpark32, B-9820Merelbeke, Belgium ("Nuance");

Developer Express Inc., a Nevada company having its place of business at 6340 Mcleod Dr. Suite1, Las Vegas, NV 89120, USA (“DevExpress”);

Pixel Translations a Division of Captiva Software Corporation, a Californian company having its place of business at 1299 Parkmoor Drive, San Jose, California 95126, USA (“Pixel”).

You understand and acknowledge that any software module included in the Software may have utility with or be able to be called by other software and/or hardware, which Spielberg considers to be an unauthorised use of the Software. Accordingly, you agree that you will use such software modules only as part of the Software and not in conjunction with, or as part of, or as a component of other software and/or hardware which makes calls to such software modules.

Spielberg grants you the personal non-exclusive rights:

For a single-user version of the Software, to install and use the Software for internal purposes only on a single computer (the Software is considered in use when it is installed in the temporary memory, i.e. RAM, or the permanent memory, i.e. Hard Disk Drive).

For a multi-user version of the Software, to install and use the Software for internal purposes only for the number of computers or simultaneous users identified in the Installation Configuration sheet of the Software package (for example, if you have purchased a 5-User license you may install the Software for simultaneous use by up to 5 Users on a network).

BACKUP COPY

You may make whatever copies you deem appropriate from the FileDirector "delivery" Compact Disc, the Programs, Example Files and any other promotional material that may be included thereon. The Application Manual, or any part thereof, may be reproduced in sufficient quantity to support only the number of users licensed to you and no more. You must reproduce and include on the backup copy the copyright notice and other ownership or proprietary legends that are on the original copy of the Software.

You may NOT make or attempt to make any copy whatsoever of the FileDirector License. ANY ATTEMPT TO COPY, TRANSFER OR RESTORE THE LICENSE MAY CORRUPT THE ENABLING LICENSE. The License, once enabled, represents the full purchase value of the license to use the FileDirector Software. The enabled License can be manipulated ONLY by the commands within the FileDirector application.

RESTRICTIONS

You may not market, distribute or transfer the Software or the Documentation to others, or electronically transfer the Software from one computer to another over a network except as expressly provided herein.

You may not de-compile, reverse engineer, disassemble or otherwise reduce the code of the Software to a human perceivable form.

You may not modify, adapt, translate, rent, lease or loan the Software or the Documentation or create derivative works based on the Software or the Documentation.

OWNERSHIP AND COPYRIGHT

Spielberg, Microsoft, Microplex, Nuance, DevExpress and Pixel reserve all rights to their respective software modules of the Software and the Documentation. The Software and the Documentation is copyrighted. Unauthorised copying of the Software, including portions thereof, or the Documentation is expressly forbidden.

EXPORT CONTROL

You agree that the Software and Documentation will not be shipped, transferred or exported into any country or used in any manner prohibited by the United States Export Administration Act or any other applicable export control laws, restrictions or regulations of the countries involved.

SUPPORT AND UPDATES

Spielberg, Spielberg's subsidiaries or affiliates, their distributors and dealers are not responsible for maintaining or helping you to use the Software and the Documentation, excepting where agreements have been entered into between specific parties, i.e. Spielberg: Distributor, Distributor: Dealer, Dealer: End User.

No updates, fixes or support will be made available for the Software and Documentation other than by publishing such revisions on the Spielberg web site: http://www.spielberg.de or http://www.filedirector.com

Any updates, fixes or support will be made available on the said web site solely at the discretion of Spielberg, who is under no obligation whatsoever so to do.

LIMITED WARRANTY AND DISCLAIMER OF INDEMNITY

Limited Warranty. The Software and documentation is provided "as is" without warranty of any kind, either express or implied, including, but not limited to implied warranties of merchantability and fitness for a particular purpose. The entire risk as to quality and performance of the Software and documentations is with you. Should the Software prove defective you (and not Spielberg, Spielberg's affiliates, their distributors or dealers) assume the entire cost of all necessary servicing, repair or correction. Some states or jurisdictions no not allow the exclusion of implied warranties, so the above exclusion may not apply to you. This warranty gives you specific legal rights and you may also have other rights which vary according to state or jurisdiction.

Spielberg, Spielberg's affiliates, their distributors and dealers do not warrant that the functions contained in the Software will meet your requirements or that the operation of the Software will meet your requirements or that the operation of the Software will be uninterrupted or error free.

However, Spielberg or Spielberg's affiliates warrants a compact disc or diskette on which the Software is stored to be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date you purchased the same, as evidenced by a receipt or otherwise. Some states or jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

CUSTOMER REMEDIES

Spielberg's entire liability and your exclusive remedy shall be the replacement of the Compact Disc and/or Diskette not meeting the LIMITED WARRANTY and which is returned to Spielberg or Spielberg's marketing affiliate, Spielberg Solutions Limited, with a copy of your receipt or otherwise. The LIMITED WARRANTY is void if failure of the Compact Disc has resulted from accident, abuse or misapplication of the software.

No liability for consequential damages. In no event shall Spielberg, or Spielberg's affiliates, their distributors or dealers be liable for any damages whatsoever (including without limitation, direct or indirect damages for personal injury, loss of business profits, business interruption, loss of business information, or other consequential or incidental damages) arising out of the software, the use thereof or inability to use the software even if Spielberg, Spielberg's affiliates, their distributors or dealers has been advised of the possibility of such damages. Some states or jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, so the above limitation may not apply to you.

Disclaimer of indemnity. Spielberg, Spielberg's affiliates, their distributors and dealers shall have no obligation to indemnify you against any claim or suit brought to you by a third party alleging that the Software or the use thereof infringes any intellectual property of such third party.

TERM

This agreement is effective upon the installation of FileDirector Server and Client and remains in effect until terminated. You may terminate this agreement by destroying the Software and any copy thereof. This agreement will also terminate if you fail to comply with any of the terms of this agreement. In addition to Spielberg enforcing its legal rights, you must then promptly destroy the Software and any copy thereof.

ACKNOWLEDGEMENT

By selecting the 'Yes, I accept the agreement' option during the software installation process, you acknowledge that you have read this agreement, understand it and agree to be bound by its terms and conditions. You further agree that this agreement is the complete and exclusive statement of agreement between you and Spielberg concerning the subject matter hereof, which supersedes any proposals or prior agreements, oral or written, and any other communication between you and Spielberg relating to the subject matter hereof. No amendment to this agreement shall be effective unless signed by a duly authorised representative of Spielberg.

Should you have any questions concerning this agreement, or if you desire to contact Spielberg for any reason, please write to your authorised supplier requesting that they pass your correspondence to Spielberg Solutions GmbH.

Table of Contents

Welcome to FileDirector

Overview

FileDirector is the complete solution for your document management requirements. The capture, classification and distribution of documents is fast and efficient, and FileDirector, as it is based on a modular system, allows you to effectively tailor your own solution, and as your organisation grows FileDirector can fully adapt to meet the demands.

The solution delivers fast and reliable capture scanning options through the enhanced connectivity between FileDirector and Canon's DR scanner range as well as support for TWAIN and ISIS scanner drivers. It's capability to perform intelligent searches makes for precise and speedy retrieval.

FileDirector has a host of standard and options features, including:

- Support for 32 or 64 bit operating systems
- Microsoft SQL or Oracle database
- Disaster Recovery site replication
- Zone and Full text OCR, Barcode and Forms recognition
- Full Audit trail
- Life cycle management
- Full version control
- Microsoft Office integration
- MailStore Microsoft Exchange Connector
- SharePoint Connector
- Codeless Integration
- SAP certified Integration
- Integrated Process Management
- Advanced Scanning tools
- Virtual Network Printer
- TIFF Image Printer
- TWAIN & ISIS Driver Support
- In built Canon Scanner Drivers

Microsoft .NET

Microsoft .NET technology allows the development of XML (Extended Markup Language) based applications, processes and Web-services. The open standard and the scalability of .NET make integration of different applications and manufacturers an easy and inexpensive task for your enterprise.

The universal approach to .NET technology makes it possible for FileDirector to be linked to other applications which also support the .NET framework.

XML- based data storage and exchange

XML has become the standard for data exchange between different platforms. Especially in document management environments XML offers wide possibilities with its capability to store index and Meta data in readable format for an enterprise wide solution. The open architecture of FileDirector in connection with XML files builds a versatile combination which expands the limits of traditional archiving. Documents are not limited to the FileDirector system - External applications can access the documents – without overstepping the security requirements.

Requirements

Supported Operating Systems

FileDirector is a Microsoft Windows based solution. The server is available for 32 and 64bit operating systems. IPv6 is supported. The following operating systems are recommended:

Server

Microsoft® Windows® Server 2003 Product family
Microsoft® Windows® Server 2008 Product family
Microsoft® Windows® Server 2012 Product family

Microsoft® Windows® Vista
Microsoft® Windows® 7
Microsoft® Windows® 8

Notes:
Windows Vista, Windows 7 and Windows 8 are only recommended for evaluation environments

Client

Microsoft® Windows® XP
Microsoft® Windows® Vista
Microsoft® Windows® 7
Microsoft® Windows® 8

Notes
Microsoft support for Windows XP ceases in April 2014. It is recommended that installations still using Windows XP are upgraded to Windows 7 or 8.
For all listed systems, Microsoft® Internet Explorer 7 or higher and Microsoft® Windows® Installer 3.0 or higher is also required.
OfficeLink supports MS Office versions from 2007

Database

FileDirector requires a SQL database server. The following database systems are supported: Where appropriate the latest service packs have to be installed.

Microsoft

SQL Server 2005 Editions
SQL Server 2008 Editions
SQL Server 2012 Editions

Oracle

Oracle9i® Editions
Oracle10g® Editions
Oracle11g® Editions

Notes
Dedicated database servers will normally result in improved performance..

Before the installation of FileDirector you must have all database components such as the Oracle database with full text installed, as it is required to configure the databases.

Licensing

Each FileDirector server installation is authorised using a licence file which contains the name of the licensee, the licence options, serial number and specific server parameters.

Serial number

The serial number is a unique, 25 character code, which is supplied upon purchase of a FileDirector system. Enter this number when running ***GetSiteCode.exe***. This will produce a Site Code file called ***serialnumber.fds***

Licensing through the Configuration Utility

Licensing the FileDirector server can be carried out using the ***Configuration Utility***.

Open the ***Configuration Utility*** on the server FileDirector is installed on. Select the ***Licensee*** tab, type in the serial number and press the ***Get licence*** button.

The Configuration Utility will then collect the licence and activate the FileDirector installation.

Obtaining a Licence using a Site Code

Copy the program ***GetSiteCode.exe*** to a directory located on the server where the FileDirector server application is installed.

Run ***GetSiteCode.exe*** and enter the serial number into the window which appears.

A file with suffix ****.fds*** is created which contains the Site Code for the server.

In your browser software, go to www.spielbergsolutions.com/fdlicence. and browse to the location where the .fds file was saved, by clicking on the ***Choose file*** button

Click on ***Get FileDirector Certificate***

The certificate for your FileDirector Installation will be created. An ****.fdc*** is generated and sent which must be saved to the FileDirector server.

In order to activate the FileDirector installation, open the ***Configuration Utility*** on the server FileDirector is installed on. Select the ***Licensee*** tab, and browse to the certificate file (*.fdc) location. Pressing the ***Apply*** button will activate the installation

Notes
After the licence file has been loaded in the Configuration Utility, it is stored in the virtual directory of the FileDirector Server (default path: \inetpub\wwwroot\filedirector).
*In addition to that a file with the name of the licence and the extension *.fda is created, which is used for VNP-licensing.*

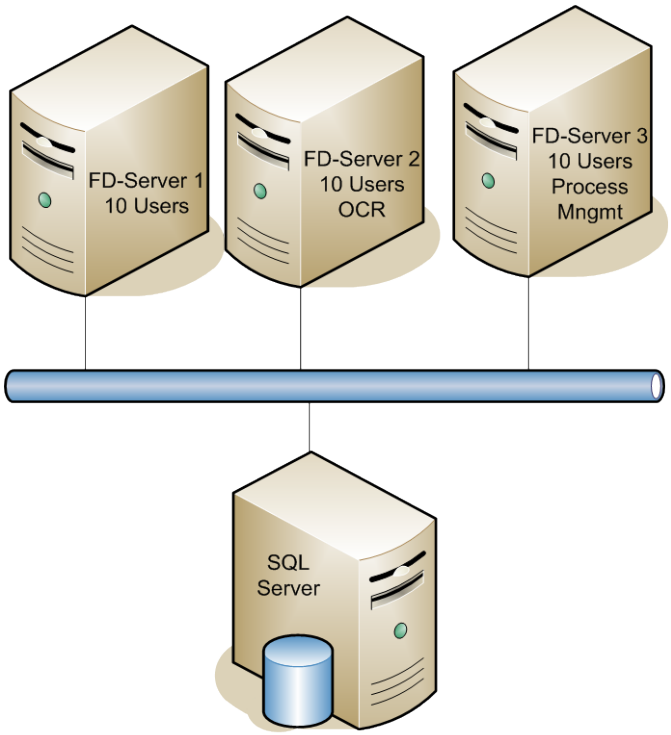
Single Server License

If you are using multiple single servers, for each server a Single Server FileDirector licence must be installed. In this model the processes which require additional resources can be configured to run on different servers. Additionally, you can spread the FileDirector user licenses over the servers.

The following example shows 3 servers. All three allow 10 users each, and server 2 has an OCR licence and server 3 has a process management licence.

The OCR scheduler can be configured to run on Server 2 and the Process Management can run on Server 3.

Example Single Server Configuration



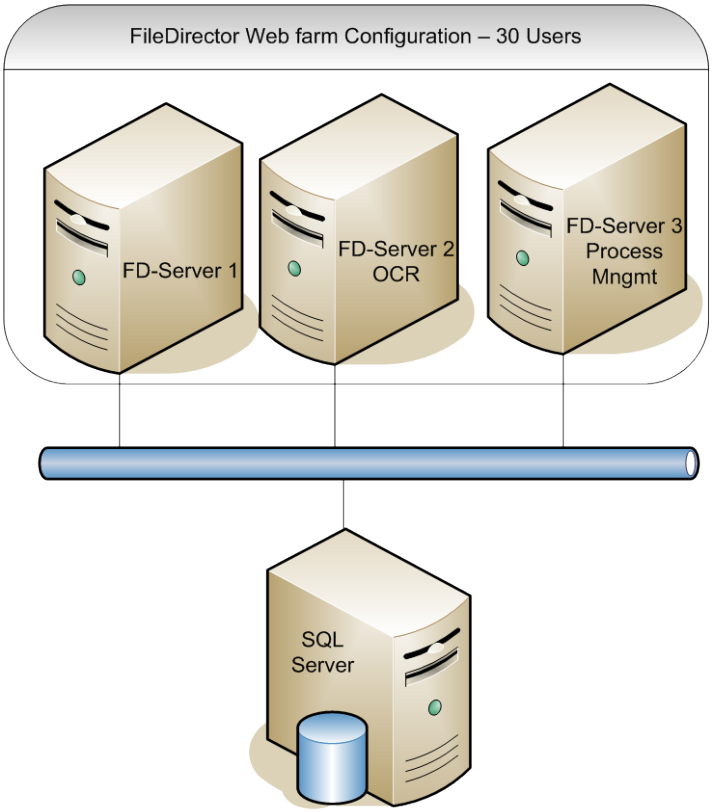
When the licences are distributed in this way, it is not possible for 30 users to connect to a single server, 10 users can connect to each of the single servers.

Web Farm License

If a Web farm licence is used, the same FileDirector licence is installed on each server in the farm.

IIS will automatically balance the load on the servers, although options such as full text OCR and process management can be configured to run on specific servers within the farm.

Example Web farm Configuration



Each user can be logged on to any of the servers, as there is an overall licence for all servers.

Server Configuration

We recommend that prior to installing the FileDirector Server application, the configuration information given below is performed, taking into account the host operating system.

Authentication

When installing FileDirector within a domain and you are intending to use Active Directory accounts for authentication, it is recommended that you are logged in to the FileDirector host server using an account with Active Directory administrative privileges. This account must also have administrative privileges for the server FileDirector is being installed to.

During a domain installation & configuration, the FileDirector user account and user groups can be automatically created in Active Directory from within the FileDirector Configuration Utility using the currently logged in account. This account must have sufficient permissions to carry that out. If the account being used does not have Active Directory administrative privileges, the FileDirector user account and user groups will have to be created manually.

If you are intending to use the FileDirector internal user accounts for authentication, you must have administrative privileges for the server that FileDirector is being installed on to.

Standard Installation Steps

1. Log on using an administrative account
2. Operating System Configuration
3. FileDirector Server Installation
4. Run the FileDirector Configuration Utility
    - Create the IIS application and application pool
    - Create the fd-server user account and user groups
    - Connect to Database Server
    - Licence FileDirector
    - Branding of FileDirector Client Applications
5. Configure the virtual directory in IIS
6. Test the FileDirector Server

If the server test is successful, the other FileDirector applications and modules can be installed. For Cabinet configuration, FileDirector Enterprise Manager has to be installed.

IIS and .NET

FileDirector requires the .NET Framework Version 4.0. On the server hosting FileDirector, IIS must be installed BEFORE the .NET framework. If this is not done, the .NET Framework should be removed from the system and reinstalled. Just reinstalling the Framework will not work.

.NET can be reregistered from the command prompt. Please check the path for the windows version before you call this command:

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe –i

Or

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe –i

Physical Server Name

The name of the server must not be the same as the FileDirector user account. By default, the FileDirector user account name is ***fd-server***.

Windows 2008 with IIS 7

User Account Control (UAC)

During the installation of FileDirector user account control must be deactivated. It can be re-activated after the installation.

You can turn it on/off via ***Start → user control → accounts → Turn User Account Control on or off.***

Notes
The Server must be restarted after turning the user account control on or off.

IIS 7

IIS 7 must be an installed role on the Windows 2008 Server for FileDirector to install and run.

IIS is installed through the Server Manager as a role.

After selecting Web Server (IIS) as a role, the following features have to be added to the Web Server role:

- Windows Process Activation Service, which contains the process model and configuration API's
- Security
    - Basic Authentication
    - Windows Authentication
    - Digest Authentication
- Application Development
    - ASP.NET
    - .NET Extensibility
    - ASP
    - CGI
    - ISAPI Extensions
    - ISAPI Filters
- Management Tools
    - IIS 6 Management Compatibility, including all its options.

.NET Framework 4.0

The .NET Framework 4.0 must be installed. This is done through the Server Manager.

FileDirector Server Installation

The FileDirector Server installation will create a program folder for FileDirector on the selected storage location of the server and installs the necessary applications and files within the folder.

Installation

To start the installation for 32bit server operating systems, run ***FileDirector Server Setup.msi*** from the FileDirector installation CD. For 64bit systems, run ***FileDirector Server Setup x64.msi.***

The server installation displays a welcome window. After clicking the ***Next*** button the ***Installation Folder*** screen is displayed. After setting the options described below, click the ***Next*** button to install the server application

Installation Location

The server application will by default be installed into the Program Files folder of the server. This can be changed if a different location is required..

Everyone or Just me

Selecting ***Everyone*** or ***Just me*** determines if the desktop icon is created for each user in start menu and on his desktop or if they are only installed for the user performing the installation.

What is installed

During the installation a program folder is created in the selected location. This folder contains the server application.

Additionally a sub folder called ***\Setups*** is created, which contains the installation files for the FileDirector client applications.

The setup files for the FileDirector client applications, such as Enterprise Manager and the Windows Client are copied during the installation,

> *Notes*
> *If the setup folders are manually copied to the installation location, ensure that they are not write protected.*

After installation an icon for the FileDirector Configuration Utility will appear on the desktop.

Scheduler Service

During the installation the ***FileDirector Scheduler Service*** is added to Windows Services. The service manages and runs the scheduled tasks configured within FileDirector.

The scheduler service will be configured and automatically started once the FileDirector server Configuration utility has been run.

IIS Configuration – Windows 2008

Once the FileDirector Server has been installed and configured, it may be necessary to alter the FileDirector virtual directory settings, depending upon how the system is to be used.

During the configuration of FileDirector a virtual directory is created in the selected web site. The name of the virtual directory is selected during installation. The default value is ***FileDirector***.

The security settings of this virtual directory may have to be changed to ensure that only authorised users have access to FileDirector. The settings required will differ depending upon whether Windows User accounts or the FileDirector internal user accounts are used for authentication.

Open the Management console for Internet Information Services:

> ***Start → Settings → Administrative tools → Internet Information Services Manager.***

FileDirector Authentication

The default authentication settings for FileDirector are ***Basic Authentication*** and ***Windows Authentication***.

Select the virtual directory of FileDirector and open ***Authentication***.

For Windows Accounts Authentication

Disable Anonymous Authentication and enable Basic Authentication and Windows Authentication.

For FileDirector Accounts Authentication

Enable Anonymous Authentication and disable Basic Authentication and Windows Authentication.

FileDirector Web Authentication

The security settings of this virtual directory must be changed to ensure that only authorised users have access to FileDirector. The settings required will differ depending upon whether Windows User accounts or the FileDirector internal user accounts are used for authentication.

For Windows Accounts Authentication

Disable Anonymous Authentication and enable ***ASP.NET Impersonation***, ***Basic Authentication*** and ***Windows Authentication***.

For FileDirector Accounts Authentication

Enable ***Anonymous Authentication*** and disable ASP.NET Impersonation, Basic Authentication and Windows Authentication.

Setups Authentication

The directory security of the virtual directory must be set to ***Anonymous Access*** for workstations on the network to install from the FileDirector Website.

Enable ***Anonymous Authentication*** and disable all other options

HTTP-Response Headers for Setups

Select ***Set Common Headers*** and set ***Expire Web content: After 5 minutes***.

HTTP-Response Header for WinCweb and EMweb

Select the respective virtual directories for WinCweb and EMWeb and select the window ***Set Common Headers*** and uncheck the option ***Expire Web content***.

Configuration Utility

Overview

The installation of the FileDirector Server will create a desktop icon for the ***FileDirector Configuration Utility***. The installation must be configured before attempting to run FileDirector for the first time.

The FileDirector Configuration Utility is used to:

- Configure server settings, such as the web site and application pool
- Specify the user account which is used by the FileDirector Server.
- Create the user group's fd-admins, fd-scan, fd-scan-named, fd-user, fd-user-named for FileDirector in the system.
- Connect FileDirector Server with SQL Server.
- Configure the default document storage location
- Define the URL from where the Client installations should be started. (Branding writes the URL in the APP.xml).
- Load the licence file.
- SMTP-configuration (Outgoing server for Emails) for sending Emails during process management

To configure the FileDirector Server double click on the ***FileDirector Config Utility*** icon on Desktop.

Server

The settings detailed below can be applied. This tab will also display the currently installed server version in the bottom right corner of the tab.

Description

You can enter a description for the FileDirector server, which by default is ***FileDirector Web Service***.

Session Timeout

In session time out (minutes) you can enter the period of inactivity after which a user's FileDirector licence will be made available for other users.

Language

Here you can select the standard language for the configuration program. When using ***Windows defined*** the language set in the operating system will be used.

Web Site

From the drop down list, you can select the web site on the server that the FileDirector server application is to be installed to.

Virtual Directory

This is the name of the virtual directory representing FileDirector in IIS. If for example the web address is www.companyname.com, access to FileDirector would be by using www.companyname.com/filedirector, if the default setting is used.

Application Pool

Select the appropriate application pool to use with the FileDirector. This can be an existing pool, or select the FileDirector pool that is listed. If this does not exist, it will be automatically created with the correct settings for FileDirector.

User and groups

The Users and Groups tab allows you to configure whether FileDirector will use Active Directory, Windows accounts or FileDirector internal accounts management for authentication. You can also set the names used for the groups FileDirector requires, as well as the user account the FileDirector server will use to access resources.

Built in Domain

Here the built in domain can be defined. Multiple ‘domains’ can be specified, with the names separated with a comma.

Account and group locations

Here the location is selected where the user account fd-server and the FileDirector-groups should be created. This can be the local workstation or a domain. If selecting several domains the fd-server account must be created on the primary domain.

Another option is to create the FileDirector groups with the same names in all domains and the fd-server account can then browse for these groups.

FileDirector Groups

During the installation the following groups are created:

fd-admins

User accounts which are added to this group have full access to all data in FileDirector. Administrators are automatically added to this group. Any member of the group can configure all options in FileDirector Enterprise Manager.

fd-scan-named

Members of this group have access to FileDirector. Within Enterprise Manager the permissions to the cabinets and document types are granted by the administrator for this group. Members of the group have no access to the system configuration even if they have all rights. With the appropriate permissions, they can manage the administrative part of the cabinets. This group can only have the same number of the members as the number of named licences purchased. Access for named users is guaranteed.

fd-scan

Members of this group have access to FileDirector. Within Enterprise Manager the permissions to the cabinets and document types are granted by the administrator for this group. Members of the group have no access to the system configuration even if they have all rights. With the appropriate permissions, they can manage the administrative part of the cabinets. Members of this group have access to a pool of concurrent licences.

fd-user-named

Members of this group are unable to scan documents. This group can only have the same number of the members as the number of named licences purchased. Access for named users is guaranteed.

fd-user

Members of this group are unable to scan documents. Members of this group have access to a pool of concurrent licences.

Server account

FileDirector will use the account specified to access the resources it requires, such as Active Directory, SQL Server and networked storage locations. No other account, including user accounts, requires any access to FileDirector data.

The fd-server account is used for a specific purpose and cannot be used as a FileDirector user account. The account will not exist in the FD-groups and will be removed when importing the accounts.

Name

The default name given to this account is fd-server, although you can change this to another name if required. You can also select the domain or local system where the account will be created.

Password

The password for the user account must be specified, and confirmed, and must be at least 8 characters in length

If the password needs to be changed at any time, this should be done using the Configuration Utility, because the password is stored by FileDirector.

Notes
The computer name of the FileDirector-Server must not be the same as the name of the FileDirector Server user account.
Accounts refresh interval (minutes)
If the permissions for imported users and groups are changed, this refresh interval is the maximum time taken before FileDirector is updated with the new permissions. The default setting is 10 minutes. When restarting IIS all updates are applied immediately.

Create FileDirector- accounts

When the configuration settings are complete, the FileDirector groups and the FileDirector user account are created in the stated domain/computer respectively.

The user ***fd-server*** is added automatically to the user group of the LOCAL administrators. This simplifies the installation when installing the database on the same computer as the FileDirector server.

If the database server is located on another server, the user ***fd-server*** must have rights to access this.

The configuration database ***FDconfig*** and the groups/accounts are created by the currently logged in user. This user must have the rights to create a database and users/groups.

The logged in user will be added automatically to the ***FD-Admins*** group.

Notes
The administrator is not automatically added to the fd-admins group. The administrator or further administrative-users can be added to the group manually.

The [domain\fd-server] user must be able to access the ADS to load the [domain\accounts] into Enterprise Manager. The accounts of the users of the domain are entered in the local fd-groups.

Database

With the options on the database tab you can connect the FileDirector server with your SQL Server and create a configuration database in the entered path. If you chose a server type, the corresponding database connection is searched.

Connection settings

The entries in Connection settings inform FileDirector about the location, type and user-account for a connection to the SQL server.

Using Microsoft SQL Server versions the instance of the standard installation is normally the same name as the server that SQL server is installed on. Enter the computer name where the SQL Server is available on, into the field name.

If an instance of SQL-Server is a SQL Express-Version, enter the name of the instance of SQL-Server: ***SQLServerName\InstanceName***

(Default instance: [server name]\SQLEXPRESS)

Define In the drop-down-list in ***Server type*** whether Microsoft SQL Server or Oracle database is used.

Notes for Oracle as server type
For the configuration of an Oracle-Database a Tablespace must be set up manually in the Oracle-Database for FileDirector.
In Oracle Enterprise Manager select Storage → Tablespaces and create a Tablespace called **FileDirector***. Set an appropriate tablespace size, as the size of the standard tablespace is only 5MB.*
Further, the **Oracle Data Provider for .NET** *must be installed on the server FileDirector is installed on.*
The name of the connection setting must be the same as the service name of the Oracle-Servers.
Full text:
The full-text-option for the database is installed automatically during the standard installation of Oracle. If the installation of the Oracle component is done after the installation of FileDirector, an update of the cabinets via the Enterprise Manager must be performed in order for an index in the FD-images table for the full text to be set.

Authentication

Connection with windows account

For the connection between SQL Server and FileDirector you can choose between integrated Windows authentication and usage of a special SQL user account.

The integrated windows authentication account fd-server is used.

Connection with SQL account:

When using a special SQL account, this account must be configured with a relevant password in SQL server.

If this connection is used, SQL server must allow this type of log in. This is set within SQL Server Management Studio Properties.

Connection pools

With Connection pooling a physical database connection can be reused and shared.

If the server accesses the database, SQL server must provide a database connection for the database operations. As the establishing of a database connection is a resource costly operation, a database is not closed immediately, after a client stops working.

If the operations with a connection are stopped, the connection is not closed but is returned into the pool of free connections. The big advantage of a connection pool against a normal database connection is that initially some connections are opened and can temporarily be provided for single clients. With this method a relatively large number of clients can work with a relatively small number of database connections.

FileDirector supports the usage of connection pools where Max. Number of connections denotes the maximum number of database connections, which FileDirector Server can establish with SQL server.

Connection time out (seconds) denotes, after which time a connection is automatically removed from the pool.

Max. Number of connections	Default value: 5
Connection time out (seconds):	Default value: 60

Max. Number of hits in hitlist

In order to limit the time for a search result, the maximum number of found documents can be limited. The default value is 1000; this value can be configured in file web.config.

See also → General administration → Settings web.config

FileDirector Configuration database

In ***default database location*** an available folder for the FileDirector configuration database must be set. The fd-server account must have full access to this location.

That also applies to the ***default storage location***. The documents in the cabinets are stored here. The storage location can also be changed individually after creating a storage location. A precondition is that the fd-server must have full access to the path.

The ***FDconfig*** database is created when the FileDirector Server is run for the first time. This can be done by performing the following steps:

- Select ***Start Run*** and enter ***IISRESET***. This will reset IIS, ensuring that all setting changes will be used.
- In a web browser, go to ***http://servername/filedirector/dataaccess.asmx***. If the configuration has been completed correctly, the FDconfig database is created in the specified path.

Before creating the database the standard storage location for documents has to be specified:

Select a folder in the window or create a new folder and click ***OK***.

If this directory is located on another server or storage medium than the FileDirector Server itself, it must be set so that the account fd-server has full control over the location.

You are then prompted for the storage location of the FileDirector configuration database (FDConfig). This can be selected from the list of available SQL storage locations. SQL server only offers storage locations already known to it. If you want to add a location to the selection, you have to create a database manually in SQL server on the new location (which can later be deleted), or the created database has to be moved.

Licensee

To licence FileDirector you will need a valid licence file. Please read the *Licensing* chapter on obtaining a License

If you have received a valid licence file with valid signature, you can load it by selecting the file using the directory browser. If it is loaded, the licence data and available options are displayed and FileDirector can be used.

Licence Options

In Licence options the licensed modules for FileDirector are displayed. A description of the single options can be found in ***Administration Guide***.

Notes
*After importing the licence file only the number of the added ticker will be displayed. The number of the available ticker can be found using **INFO** in the WinClient.*

Branding

Using Branding, the URL which a FileDirector client needs to connect to the FileDirector Server can be set. This path is stored in the file ***APP.XML*** which is located in the relevant folder in SETUPS located under the virtual directory of FileDirector.

\inetpub\wwwroot\filedirector\Setups\[application name]

If branding is not performed, the clients cannot be installed using a browser and the installation page, because the relevant *.msi file for installation will not be found.

Notes
If the server or files in the Setups folders are updated, branding has to be performed again.

Server URL

This field stores the URL of FileDirector Server which is called by the clients. After installation all client requests to the server are processed using this address.

Automatic log-in

When ***Automatically log-in using current windows account*** is used, The WinClient and Enterprise Manager will start without having to type in a user name and password. The information of the windows account currently logged in is used.

SMTP-Server

SMTP is an abbreviation for ***Simple Mail Transfer Protocol***. This protocol controls sending emails t. The File Director Process Management option can send emails with a link to the document to be processed. For this option the SMTP address of the email server must be specified. The default port is 25.

FileDirector system notifications can be configured to be sent to an email address. Enter a notification description in ***Message from***: and the recipient email address in ***System Notification recipient***.

In order to test the server address, valid email addresses can be typed into the fields ***Message to*** and ***Message from***. A test mail is sent via the server when ***Test it*** is clicked.

Web-Server URL

If an Email is sent via the Process Management option of FileDirector and the relevant document should be viewed using WebServer, specify where WebServer located.

Test installation

The server installation and configuration should be tested to check that everything is installed and configured correctly.

Open a browser window and specify the following virtual FileDirector address:

http://localhost/filedirector/dataaccess.asmx

For ***[localhost]*** the name of the FileDirector Server must be entered.

If IIS and FileDirector are configured correctly, a list of functions used by the FileDirector Server is displayed.

Connection test

Using the function ***TestConnection*** log-in to IIS can be checked.

Click on ***Invoke*** on this page in order to check the connection to the FileDirector Server.

If this test is successful, an XML page should be returned and displayed, which shows the account currently logged in, for example:

…Welcome domainname\administrator on server server name…

Notes
*If for example **Anonymous** or the local name of the server is returned, either the log-in is wrong or the security settings in IIS are not configured correctly.*

Test database access

To check if FileDirector has access to the database, a further step is required. If database access fails, the WinClient and Enterprise Manager cannot establish a connection to the server. This test should principally be executed after the installation and upgrade of FileDirector Server.

While searching for malfunctions and errors this test is helpful, if the applications cannot establish a server connection. This test ensures that the server is configured and operational.

Select ***Get Cabinets***; enter ***true*** into the field ***Value*** and then ***Invoke***.

Even if no cabinets have been created, this information will be requested from the database and displayed in an XML page:

The Installation and configuration of FileDirector Server is complete. FileDirector Enterprise Manager can now be installed.

If an error message appears during these tests, the server must be checked again with the points listed previously. If the server is not configured and working correctly, applications such as Enterprise Manager and WinClient will have problems connecting to the server.

Manually Create Groups and Account

During the configuration of the FileDirector Server the Configuration Utility normally creates the following accounts and groups in the domain:

Account: fd-server (+ Password)

Groups : fd-admins

fd-scan

fd-scan-named

fd-user

fd-user-named

This requires that the account used when running the Configuration Utility is a domain administrator, and is allowed to create users and groups in a domain.

If it is not possible to log in as a domain administrator, these groups and account can also be created manually by a domain administrator.

The fd-server account must be a member of the domain users group and must be a member of the local administrator group of the FileDirector Server.

Once the account has been created, start the Configuration Utility, and enter the account name and password within the ***User & Groups*** tab. The password is stored encrypted in the file web.config.

After specifying these settings restart IIS on FileDirector Server and check access using ***/dataaccess.asmx/GetCabinets*** with Internet Explorer.

Security settings for database access

If the login to SQL server is done using windows authentication, the fd-server account is used.

Example 1:

SQL-Server and FileDirector Server are installed on the same server and windows authentication is used.

As the ***fd-server*** user account is a member of the local administrators group, it will also have access to the SQL server.

Default settings in SQL-Server:

Security → Accounts → BUILTIN\Administrators → Properties → \|server rolls\| → ☑ System Administrators

Example 2:

SQL-Server and FileDirector Server are installed on the same server and authentication via SQL is used.

If the user ***sa*** is used in the default settings, this account is configured as system administrator.

Default settings in SQL-Server:

Security → Accounts → sa → Properties → \|Server rolls\| → ☑ System Administrators

If minimum rights are to be granted, the account used (which need not be sa) must have a minimum of ***Database creator*** permissions.

Security → Accounts → (enter SQL user) → Properties → \|Server rolls\| → ☑ Database creators

Examples 3 & 4:

SQL server and FileDirector Server are installed on different servers.

If the fd-server account should access SQL-server with windows authentication and minimum rights, fd-server must be entered to the server rolls of the database server.

In SQL server this account must at least be entered as database creator to grant access to the databases created by fd-server.

These settings are performed in the Enterprise Manager of SQL server:

Using windows authentication:

Security → Accounts → (enter fd-server) → Properties → \|Server rolls\| → ☑ Database creators

Using login to SQL:

Security → Accounts → (enter SQL user) → Properties → \|Server rolls\| → ☑ Database creators

All databases, which are created in Enterprise Manager, are created by the user specified in the Configuration Utility and get access to the databases created. Access to other database created by another account, must be manually accessed.

Security → Accounts → (select user) → Properties → | Database Access | → Select Databases (FDConfig, FD_xxxCabinets)

Problems during server testing

Documents cannot be checked in

The system time of clients must not differ more than 5 minutes from the server system time otherwise the server will refuse to check in documents.

Mandatory fields were not filled

The connection to the server is disconnected (network problem)

The storage pool is false, full or the access for fd-server is not allowed.

Setting of storage pool

Server message: No valid storage pool data found.

If this message appears when checking in documents from the WinClient, the settings or access rights of the storage pool is not OK.

Check if the storage pool points to a valid directory and if this directory is accessible for account fd-server.

Error during server check (GetCabinets)

If an error appears during checking of the server, this may come from access with account ***fd-server***. The following settings should be checked (more detailed information can be found in the respective sections):

The fd-server account password must conform to the rules of the host domain/operating system, and must have been entered correctly in the Configuration Utility.

- Was log-in performed as domain administrator when installing FileDirector Server?
- Have fd-groups and account fd-server been successfully created?
- Are the settings of IIS correct? (Test Connection)
- Has the database ***FDConfig*** been successfully created and have the accounts been imported correctly into the table ***Accounts***?

Notes
Even if no cabinets have been created, the server test can be carried out using **GetCabinets**. *If there are no errors, this information is also returned in an XML file.*

WebServer

Using FileDirector WebServer you can easily access documents held in FileDirector through a browser without having to install additional client software.

FileDirector WebServer allows you to view and edit existing documents, create new documents by file upload or scanning using the WebScan client and an attached scanner. In addition, users can use their inbox and FileDirector Process Management.

Access to documents is by user account authentication, configured within FileDirector. FileDirector WebServer also allows anonymous and guest user access via user accounts configured to allow access to specified documents.

Requirements

Server

FileDirector WebServer can be installed on following operating systems:

- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

To install FileDirector WebServer on one of the above operating systems, additional components are required:

- Microsoft Internet Information Services (IIS) – version 6 or higher
- Microsoft .Net Framework 4

FileDirector WebServer needs approximately 10MB of disk space. Take into consideration that additional disk space is needed for the programs document cache. For more information see *Cache Configuration*.

Client

FileDirector WebServer gives access to your documents on an intranet or the Internet. Clients can access WebServer using one of the following browsers:

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome
- Opera
- Safari
- Any W3C compliant browser

Notes

To use FileDirector WebServer's full functionality, it is recommended to keep your browser up to date. This will also increase the general security of your system when using the internet.

WebScan

WebServer allows users with the appropriate permissions to create documents. For this purpose the WebScan Client is used. This client offers a simple way to scan documents with a connected scanner or to upload files from file system directories. These files are sent to WebServer and can then be indexed.

The WebScan Client is distributed to clients as a Click-Once solution and is started directly from the web browser. The following requirements must be met:

- Microsoft .Net Framework 3.5 or higher
- One of the following browsers:
  - Microsoft Internet Explorer
  - Mozilla Firefox (Add-on: Microsoft .Net Framework Assistant)
  - Google Chrome (Add-on: Click-Once for Google Chrome)

Notes
The browser add-ons can be acquired and installed through the respective browser's add-ons option. Additional help concerning the installation procedure can be found in your browser's help file.

Creating a new Application Pool

Before WebServer is installed, create an Application Pool for the program in IIS (Microsoft Internet Information Service). This will increase security and will protect other applications hosted by the IIS. If an Application Pool is shared, configuration changes in WebServer will cause IIS to restart the Application Pool automatically, causing other applications to be temporarily unavailable.

Notes
Create an Application Pool for FileDirector WebServer use only.

Create an Application Pool (IIS 6)

A new Application Pool is created within IIS Manager. To open the IIS Manager, select ***Control Panel -> Administrative Tools -> Internet Information Services (IIS) Manager.***

Expand the nodes on the left hand side, open the context menu for ***Application Pool*** and select ***New -> Application Pool***.

Enter a unique and descriptive Application Pool ID and create the new Application Pool with ***Use default settings for new application pool*** selected.

Now set the identity of the new Application pool. Open context menu for ***Application Pool*** and select ***Properties***. IIS 6 predefines ***Network Service*** as the identity for new Application Pools. This needs to be changed, since WebServer requires additional access rights. Select the ***Identity*** tab and select ***Predefined*** and choose ***Local System***.

Create an Application Pool (IIS 7.x)

To start IIS Manager, select ***Control Panel -> Administrative Tools -> Internet Information Services (IIS) Manager.***

Expand the nodes on the left hand side of the IIS Manager window, open the context menu for ***Application Pools*** and select ***New -> Application Pool***.

Enter a unique and descriptive Application Pool ID. Select .NET Framework Version ***.NET Framework v4.x***, and set ***Managed pipeline mode*** to ***Integrated.*** Press ***Ok*** create a new Application Pool.

Any new Application Pool in IIS7.x is equipped with ***ApplicationPoolIdentity*** by default. This is sufficient and does not need to be changed.

Install FileDirector WebServer

After the Application Pool has been created, the preparations for the installation of FileDirector WebServer are completed. Start the installation file for FileDirector WebServer for your system and follow the instructions on the screen.

The installation process will need some information about your system.

If your IIS contains no special configuration, install as ***Default Web Site***. In this case use the virtual directory ***FileDirector/Web*** to install WebServer as a subdirectory of the FileDirector server. ***Application Pool*** should be set to the newly created Application Pool.

Confirm your selection by clicking on ***Next*** to start the installation process.

As part of the installation a new ***virtual directory*** is created in the IIS and the files necessary to run WebServer are copied into this directory. In addition, the ***FileDirector WebServer Config Utility*** is installed to the program directory and a link is placed on the desktop. The ***Config Utility*** is needed to configure WebServer after installation.

FileDirector WebServer Configuration

After a successful installation, IIS and WebServer must be configured before use.

Since the configuration procedure of IIS differs between the various versions, the following instructions distinguish between IIS version 6 and IIS version 7.x. Please make sure that you are using the correct configuration steps for your IIS version.

Start the ***FileDirector WebServer Config Utility*** to apply basic settings. Go to the ***WebServer*** tab and enter a valid FileDirector Server address. This allows WebServer to establish a connection to the FileDirector server. If the FileDirector Server and WebServer are installed on the same system, the FileDirector Server address is usually *http://localhost/filedirector*.

Continue with the cache configuration.

Cache Configuration

The cache is required to temporarily store data received from the FileDirector Server. In addition, a user account (cache user) with read and write permissions to the cache directory is required. This is configured using the FileDirector WebServer Config Utility.

Cache Directory

Data received from the FileDirector Server is temporarily stored in the cache directory. By default the following directory is used:

C:\Windows\Temp\FileDirector\Web

The cache directory can be configured using the ***FileDirector WebServer Config Utility***. Start the WebServer Config Utility and open the ***WebServer*** tab. The option ***Cache Directory*** contains the current cache directory path used by WebServer. This path can be changed at any time.

Notes
It is advisable to use a local drive for security and performance reasons. If the cache directory is on a network drive, the FileDirector Component Service needs additional configuration. For more detailed information about this topic, see FileDirector Component Service.

The content of the cache directory is managed independently by WebServer. Redundant data is removed automatically after a user session has been terminated.

The disk space for the cache directory is dependent on the use of WebServer and can vary greatly. If WebServer is used by many users at the same time, the disk space required increases. The used disk space decreases when the number of simultaneous users decreases.

Notes
The required disk space varies by the type of use. For example: a user retrieving a lot of documents requires more temporary disk space than a user retrieving documents sporadically. A safe prediction for the amount of disk space required for the cache directory is therefore not possible.

Cache User

WebServer needs the cache user account to be able to read from and write to the cache directory. The user account used for this is specified in ***WebServer Config Utility***.

Any account with the appropriate read and write permissions for the cache directory can be used as a cache user. For security, we suggest that you create a new user account for this purpose. If the cache directory is pointing to a local drive a local user account will suffice. The permissions of the cache user can be restricted further in order to increase the security of the system. For more information, see *Increasing the security system*.

Notes
If you use a cache directory on a network drive, the cache user account requires the appropriate permissions. The use of network drives is not recommended for security and performance reasons!

IIS 6 Configuration

The settings below apply to ***IIS 6*** only. If you use a later version of IIS, skip this section and continue with *Authentication Settings*.

To open IIS Manager, select ***Control Panel -> Administrative Tools -> Internet Information Services (IIS) Manager.***

Expand the nodes on the left hand side, then open context menu for the virtual directory ***Web Sites -> Default Web Site -> FileDirector -> Web*** and select ***Properties.***

First, set up the ASP .NET version. Change to the ***ASP.Net*** tab and set ***ASP .NET version*** to ***version 4.x***. This should always be your first step, because it affects other settings and procedures.

Once the correct ASP.NET version is set, the next step is to configure a ***wildcard application mapping***. Select the ***Virtual Directory*** tab and click on ***Configuration*** to edit the application configuration.

Add a ***wildcard application mapping*** by clicking ***Insert***.

Enter the path to the ***aspnet_isapi.dll*** file into the ***Executable*** text box. This file can normally be found in the directory:

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll

Notes
If the correct ASP.NET version has been selected and saved, you can copy the path from the .aspx application configuration. Please ensure that the correct version (v4.x) is always referenced.

In addition, the option ***Verify that file exists*** has to be deselected. If this option is selected, the FileDirector WebServer will not be started upon requests and is therefore not accessible.

The configuration of the FileDirector Webserver's virtual directory is complete. Close the Properties window to proceed to the final step.

Select the node ***Web Service Extensions*** and ensure that the web service extension ***ASP.NET v4.x*** is set to ***Allowed***. Otherwise all requests to WebServer are denied by IIS.

Authentication Settings

WebServer offers different authentication methods. ***Forms authentication*** is used by default after installation.

Depending on the required form of authentication various authentication methods have to be enabled or disabled for the virtual directory.

Even if you want to use the default forms authentication for your system, please check your configuration, using the corresponding manual sections, in case additional settings have to be applied.

Notes

WebServer can only be configured for one of the authentication methods, because the authentication settings in IIS exclude each other. For example: it is not possible to use an integrated Windows authentication for domain users and a forms authentication for external users at the same time. In this case the forms authentication has to be used for all users.

Windows Authentication

Windows authentication uses the Windows domain account used to log on to Windows, to access WebServer. The user will be automatically logged in to WebServer. In this case the login screen of WebServer is not displayed. A log-on using a different user account is not possible.

Notes
The integrated Windows authentication is tied to the use of Windows domain accounts. It cannot be used with internal FileDirector user accounts.
Since the log-on always requires a valid Windows domain account for authentication, this type of log-on is usually configured for an intranet installation.

IIS 6 – Settings

The ***integrated Windows authentication*** settings are configured with the IIS Manager. Go to ***Control Panel -> Administrative Tools -> Internet Information Services (IIS) Manager.***

Select the virtual directory of the FileDirector WebServer (***Web Sites -> Default Web Site -> FileDirector/Web***), open the context menu and select ***Properties.***

Go to ***Directory Security*** tab and click on ***Edit*** in the ***Authentication and access control*** section. Select ***Integrated Windows authentication*** and deselect all other settings, including ***Enable anonymous access***. Click on ***OK*** to apply settings and to close the window.

Change to ***ASP.NET tab*** and click on ***Edit Configuration***. The ***ASP.NET Configuration Settings*** window is displayed. Select the ***Authentication*** tab and switch ***Authentication mode*** to ***Windows***.

Save settings and restart FileDirector WebServer Application Pool.

IIS 7 - Settings

The ***integrated Windows authentication*** settings are configured within IIS Manager. Go to ***Control Panel -> Administrative Tools -> Internet Information Services (IIS) Manager***.

Select the WebServer virtual directory (***Web Sites -> Default Web Site -> FileDirector -> Web***) and open the authentication settings using ***Authentication*** on the right hand side.

Enable ***ASP.NET Impersonation*** and ***Windows Authentication.*** Disable all other settings

Restart the FileDirector WebServer Application Pool to ensure the changes have been applied.

Forms Authentication

Forms authentication is defined after installation. Upon opening WebServer a log-on form is displayed. A user can log-on with a valid user name and password.

> *Notes:*
> *Forms authentication can be used with Windows domain accounts as well as internal FileDirector accounts.*

IIS 6 – Settings

The ***Forms Authentication*** settings are configured within IIS Manager. Go to ***Control Panel -> Administrative Tools -> Internet Information Services (IIS) Manager.***

Select the WebServer virtual directory (***Web Sites -> Default Web Site -> FileDirector/Web***), and open the context menu and select ***Properties.***

Select the ***Directory Security*** tab and click on ***Edit*** in the ***Authentication and access control*** section. Select ***Enable anonymous access*** and deselect all other settings. Click on ***OK*** to apply settings and to close the window.

Change to the ***ASP.NET tab*** and click on ***Edit Configuration***. The ***ASP.NET Configuration Settings*** window is displayed. Select the ***Authentication*** tab and switch ***Authentication mode*** to ***Forms***.

Save settings and restart the WebServer Application Pool.

IIS 7.x - Settings

The ***Forms Authentication*** settings are configured within IIS Manager. Go to ***Control Panel -> Administrative Tools -> Internet Information Services (IIS) Manager***.

Select the WebServer virtual directory (***Web Sites -> Default Web Site -> FileDirector -> Web***) and open the authentication settings using ***Authentication*** on the right hand side.

Enable ***Anonymous Authentication***, ***ASP.NET Impersonation*** and ***Forms Authentication.*** Disable all other settings

Save settings and restart the WebServer Application Pool.

Anonymous Access

Anonymous access in WebServer allows users to access documents without having an account. Anonymous users are logged-on with a standard account, which is used for all anonymous users. This account is a normal user account, whose rights can be configured within FileDirector Enterprise Manager.

WebServer can use two types of anonymous access: ***Public*** and ***Guest***.

When using Webserver with a ***public access,*** the user is not asked for credentials and all users are logged-on automatically with the predefined anonymous user account. Logging-on with a different user account is not possible.

If a ***guest account*** is used, the log-on form is displayed. In addition, a ***Guest*** button is displayed on the form. The user can use their own account, log-on anonymously by clicking ***Guest***. When logging-on as guest, the user is not asked

for credentials and the log-on process is executed using the predefined anonymous user account.

To use WebServer with one of the two anonymous access types, you have to configure ***Forms authentication***. Please follow the instructions in the relevant section of *Forms Authentication*. Afterwards, restart the ***FileDirector WebServer Config Utility*** and go to ***Accounts*** tab. Select ***Allow anonymous access*** and enter the user name and password. Choose between ***Public*** or ***Guest*** access type.

Notes
Ensure that the selected user account is a valid FileDirector user and a member of corresponding FileDirector user groups.

Enhancing System Security

The following section describes settings which increase the security of your system. These settings are ***optional***. WebServer is fully operational without these settings and has sufficient security.

The settings are examples for Windows Server 2003 and Windows 7. They can be applied to other Microsoft Windows operating systems.

Notes
If you want to apply these settings, it is strongly recommended to create a separate account for the cache user. This will prevent possible side effects on other areas where the account is used.

Edit Local Security Settings

The steps below will stop the cache user account logging on interactively and allow the account to log-on as a batch job only. Once set, it is no longer possible to log-on to the system with the cache user's account. In case of an unauthorized access this restriction circumvents a direct log-on and prohibits an access to other system components.

Windows Server 2003

To edit the cache user's permissions, open ***Control Panel -> Administrative Tools -> Local Security Policy.***

Select ***Security Settings -> Local Policies -> User Rights Assignment.*** On the right hand side you'll find policies ***Log on as a batch Job*** and ***Deny log on locally.***

Add the cache user's account to both security policies.

Windows 7

To edit the cache user's permissions, open ***Control Panel -> Administrative Tools -> Local Security Policy.***

Select ***Security Settings -> Local Policies -> User Rights Assignment.*** On the right hand side you'll find policies ***Log on as a batch Job*** and ***Deny log on locally.***

Add the cache user's account to both security policies.

Adjust Configuration File (web.config)

After restricting the cache user's permissions using security policies, the WebServer configuration file has to be adjusted. The change affects WebServer's internal log in of the cache user. Open the file ***web.config*** in the FileDirector WebServer installation directory and search for:

```
<add key="FDServerLogonType" value="" />
```

Change key value to ***batch***.

```
<add key="FDServerLogonType" value="batch" />
```

Save the changes and restart WebServer Application Pool in order to apply the changes.

Notes
If you do not use a separate account as the cache user, take into consideration that the applied restrictions can affect other areas where the account is used.

Remove Group Membership

To restrict the rights of the cache user account further, its memberships in the local system's user groups can be removed. The user account will lose all access permissions to the system. The user account needs to be have appropriate permissions applied for the cache directory, since it will no longer have access to local files and directories.

If all group memberships are removed and only access to the cache directory is granted, any risk in the event of unauthorized access is minimized.

FileDirector Component Service

Not all stored document formats can be displayed in a web browser. For those formats not supported, WebServer has to process and convert documents in order to display them. For this purpose, FileDirector Component Service is required. The service needs to be installed and started on the server that has WebServer installed.

> *Notes*
> *It is not sufficient to install FileDirector Component Service on the system. The service needs to be started in order to convert files for WebServer. Usually the FileDirector Component Service is automatically started after installation, and no further configuration is necessary.*

If WebServer uses storage on a network drive, additional configuration is necessary. In this case, ***FileDirector Component Service*** needs to be started with a user account which has access to the network drive. By default, Windows will start a service with the Local System account, which has no network privileges and won't be able to access the cache directory.

Installation of Applications

General Information

FileDirector Client applications can be run in two ways; as traditional windows applications, or via a web browser.

Conventional Client installation

This can be done from the installation page or by independent software rollout. From the FileDirector installation page the applications can be installed and this would allow a user to work within the client applications when not connected to the FileDirector Server.

Web installation

The Windows Client and Enterprise Manager can be started directly from the server within a web browser. Using the browser versions allows for easier maintenance of the solution, updates and upgrades have to be applied on the server only, rather than on all the clients. The browser clients must always be connected to the server.

The client installation for use via a browser is described in the chapter *WebServer Installation*

.NET Framework

Microsoft .NET Framework 2.0 must be installed before the FileDirector applications can be installed.

Install Applications

During installation you need be logged-in as an administrator or with administrative rights.

FileDirector installation page

During the installation of FileDirector Server the setup files for all FileDirector applications are copied to the installation directory (located in \inetpub\wwwroot\filedirector\Setups\). The setups can be accessed by a web page on the FileDirector Server. The installation of Clients can be carried out from this page.

For example if FileDirector is installed to server ***[Server name]*** and to the virtual directory ***FileDirector,*** the address is:

http://[Servername]/filedirector

Enterprise Manager

Enterprise Manager is the administrative application for FileDirector. Cabinets and storage structures can be configured according to the required specifications. This application can be installed on the server and on workstations.

The account which uses Enterprise Manager for all administrative tasks must be a member of the group ***fd-admins***. For configuration of Cabinets alone a member of the groups ***fd-scan*** or ***fd-scan-named*** is sufficient, if these groups are given full cabinet rights.

- Select ***Install*** for Enterprise Manager and execute the installation from here.
- The first window shows that the file setup.exe was found for installation. Click to Open. If you are asked for a signature, confirm with ***Yes.*** Continue with ***Next*** in the next window.
- Afterwards an installation path can be selected.
- Selecting ***Everyone*** or ***Just me*** determines if the start icon is created for each user or if it is only available for the user performing the installation.
- With ***Disc Cost*** you can display the available storage capacity and figure out, the amount of storage space needed for the application.
- The installation will start when ***Next*** is selected.

Enterprise Manager can now be used for the creation and configuration of FileDirector Cabinets.

Timeout-Settings in Enterprise Manager

For the transfer of data from FileDirector Enterprise Manager to the server a time out period is utilised. If the Enterprise Manager does not receive a response from the server in the specified time frame a timeout is displayed. If the Enterprise Manager gets a subsequent response, it cannot be processed.

To change the time out period for the Enterprise Manager, a value in the file ***app.xml*** of the Enterprise Manager can be set. This file is located in the program path of the Enterprise Manager.

The following key can be found in ***app.xml*** with the default setting of ***180***:

<add key="TimeOutSecs" value="180" />

WinClient

Setup Customer- Logo

In the WinClient a logo is displayed in the control box. This logo can be stored for standard installations and is stored in directory ***FileDirector\Setups\FileDirector WinClient*** as the file custlogo.gif. If you exchange this file with your own logo file, this will be displayed after installation.

If a logo file is exchanged after installation, it must be replaced in the directory ***Program Files\Spielberg Solutions GmbH\FileDirector\WinClient*** on the relevant workstation.

An individual logo for each cabinet can be stored. If a logo is stored at cabinet level, it takes precedence over the logo selected during installation.

A logo at Cabinet level is specified in Enterprise Manager. See the section about Cabinet configuration in the Administration guide.

Installation

- Select ***Install*** for WinClient and execute the installation from here.
- The initial window will open, click ***Next*** to continue. If you are asked for a signature, confirm with Yes.
- The installation path for the WinClient can be selected, or the default location accepted.
- Selecting ***Everyone*** or ***Just me*** decides if the start icon is created for each user in the start menu and on the desktop or if they are only available for the user performing the installation.
- The installation will start when ***Next*** is selected.

PlugIns for WinClient

For the WinClient different Plugins are available, which have to be copied manually to the relevant workstation into the installation directory Program files\Spielberg Solutions GmbH\FileDirector WinClient\. For more information see the WinClient user manual.

Password with basic authentication do not store

If basic authentication is configured for the WinClient, the login window appears when the program is started. With the checkmark the password can be saved for the next login. If the option to save the password is not offered, the WinClient can be started with the parameter ***/hidesavepassword.***

To start the program with this parameter create a new link to the file ***FileDirector WinClient.exe*** which is in the program folder of the WinClient and write the parameter in the properties of the link after the path to start the WinClient. When the WinClient is started with this link, the login window appears without the checkmark box to save the password.

Timeout settings in the WinClient

For the transfer of data from the WinClient to the server a time out period is utilised. If the WinClient does not receive a response from the server in the specified time frame a timeout is displayed. If the WinClient gets a subsequent response, it cannot be processed.

To change the time out period for the WinClient a value in the ***app.xml*** file of WinClient can be set. This file is in the program path of the WinClient. The following key with the default setting of ***120*** can be changed:

<add key="TimeOutSecs" value="120" />

Component Service

FileDirector Component Service contains the Office Link. Office link is integrated into Microsoft Office products and allows documents to be saved directly into FileDirector from these applications.

With the Component service the Document Viewer is installed which allows users to display electronic documents and create thumbnails of electronic documents. With the Viewer many different document formats can be displayed, without the originating application having to be installed.

- Select Install for Component Service on the web page
- The initial window will open, click ***Next*** to continue. If you are asked for a signature, confirm with ***Yes***.
- Afterwards an installation path can be selected. This path is later automatically used for the installation of the OCR engine.
- Selecting ***Next*** will complete the installation.

Notes
*If the Component Service is installed with the option **Just me** the button in the Office Application only exists for the user who installed the Component Service.*

OCR Engine

The OCR recognition is used for configuration of full text recognition and zone recognition including forms recognition. The forms are configured with the OCR module in Enterprise Manager. The configuration covers the zone configuration, with which document types the zones are linked and which index fields should be read.

To configure OCR recognition in Enterprise Manager the OCR engine must be installed on the work station. OCR engine can only be installed if Component service is installed.

Notes
To be able to use OCR functionality a valid OCR licence is required!

Install OCR Engine on Server

For OCR recognition two modes must are available:

- Full text recognition
- Forms recognition

The OCR engine must be installed on the server if full text recognition is to be performed. Full text recognition is run on the server by a scheduler and must be configured in the database server as well. Configuration is described in the Admin guide.

For file imports using zone recognition run on the server, Component Service and the OCR Engine must be installed on the server.

Install OCR Engine on Client

If zones for indexing should be read by OCR during scanning, the Component Service and OCR engine must be installed on the client work station.

- Select ***Install*** for OCR Engine and execute the installation from here.
- The first window shows that setup.exe was found for installation. Click to Open. If you are asked for a signature, confirm with ***Yes***. Continue with ***Next*** in the next window.
- During this installation no path can be specified, because the installation path is derived from the Component Service installed initially. Finish the installation by clicking ***Next.***

Different OCR Engines

Western OCR Engine

In the installation procedure described before (from the web page) the western OCR Engine is automatically installed. This installation supports the western languages

English, German, French, Dutch, Spanish, Italian, Greek and Russian.

Asian OCR Engine

For recognition of Asian languages a special OCR Engine must be installed, which needs its own licence. It must be activated in the FileDirector licence file. Additionally a licence code from Nuance is needed for the engine itself.

Audit trail for the OCR Engine (IPRO Engine)

With the OCR Engine the service OCR Engine is installed. If an error occurs with the OCR Engine, the errors are recorded in the Windows event log.

Configure OCR Engine to one processor

In the configuration file for the OCR engine, the parameter ***process affinity*** is used to configure the processors used by the OCR process. This may have to be amended if there are issues with the OCR recognition.

The ***FileDirector OCR Engine.exe.config*** file is in the following path:

> ***\Program Files\Spielberg Solutions GmbH\FileDirector Component Service\OCR Engine***

Very occasionally multiprocessor systems can cause problems with performance and delays with OCR reading.

0	=	All processors
1	=	First processor
2	=	Second processor
3	=	First and second processor
4	=	Only on processor 3
5	=	First and third processor

Notes
Rule to configure the binary parameter: 1,2,4,8,16,32
(that means **4 = 3***. position = 3. processor e.g. with 4 processors the scale is up to 1,2,4,8… now the numbers are summarised … 1(first) + 4 (third)= 5*

ISIS Add-on

By default the WinClient supports Canon and Plustek document scanners directly via integrated drivers and other scanners via TWAIN. A FileDirector ISIS Add-on can be integrated into the WinClient which offers support for scanners with ISIS drivers.

In order to use this option a licence is required.

Select the link ***Install*** for ISIS Add-on and execute the installation from here.

As soon as installation starts a welcome window is opened. Click ***Next*** and the window where the installation can be started opens. Selecting ***Next*** will complete the installation.

Installation Issues

Msi - File could not be found

Possible reasons for the application installer file not being found are:

- Check security settings in IIS for directory \Setups
- Branding was not carried out (also after update).
- Directory FileDirector\Setups\ does not contain the setup for this application, because the server setup was started from a location, where no subdirectory \Setups was present.
- The file App.xml is write-protected because it was copied manually from a CD to directory \Setups.

APP.XML or custlogo.gif cannot be found

A file called ***App.xml*** is located in each application subdirectory.

If only the *.msi file was copied into a directory and started from there it will search for file App.xml. The installation file should always be started from a complete setup directory of the relevant application.

The WinClient setup directory must contain the custlogo.gif file.

Web installation of the applications

It is possible to install the applications (WinClient and Enterprise Manager) on the server to enable their use within a browser. Internet Explorer 6 or above and the .NET Framework 2.0 are required to be installed on the clients.

Branding

Before the installation the branding must be run in the Configuration Utility with the correct URL to the server. During installation the setups of applications must be found in the folder: inetpub\wwwroot\filedirector\setups.

During the branding the URL of the server is set to the file app.xml in the section <appSettings>:

<add key="ServerURL" value="http://servername/filedirector" />

Installation of the applications in the IIS

After running the correct branding the Installation can be executed. First run the normal setup on the server. During this process the application, e.g. WinClient is installed in the program path. Create a folder ***WinCweb*** in the virtual folder of FileDirector:

C:\Inetpub\wwwroot\FileDirector\WinCweb

All installed files can be copied from the program path C:\Program Files\Spielberg Solutions GmbH\FileDirector WinClient in the folder WinCweb.

Security settings in IIS

Under normal circumstances security settings in the Internet Information Server settings are transferred from the virtual folder of FileDirector (windows authentication and basic authentication).

See → *IIS configuration*

Add trust

To start WinClient on the client machine .NET Framework version 2.0 must be installed on the client. In addition to that the security settings must be configured so that the client can work with the FileDirector. For this purpose a trust must be added. Invoke the Installation page http://server name/filedirector and run the command ***Add trust to this site to allow execution of browser based applications*** from the top of the site.

Run Applications

After the WinCweb folder is created and the installation files of the WinClient are copied, the client can be started from the installation page - ***http://servername/filedirector***.

For the WinClient and Enterprise Manager, the option ***start in browser*** is available, which will open the following URL's:

For WinClient: ***http://servername/filedirector/wincweb/default.htm***

For Enterprise Manager: ***http://servername/filedirector/emweb/default.htm***

Notes
For Enterprise Manager use the same procedure as described for the WinClient. Here you just have to create the folder /EMweb.

If no page is displayed when attempting to open one of the pages please check the following settings:

- .NET 2.0 was not installed correctly
- Does the WinCweb folder exist and is it at the correct location
- Are the security settings in the IIS correct
- Was the branding run before the WinClient installation? Does the server URL in the app.xml exist
- Was the trust activated AFTER the URL of the server was written to the app.xml
- The date for http-header ***content expires*** was activated and must be unchecked. See *http Response Header Setting for WinCWeb/EMWeb*

Installation Manager

Advantages of the Installation Manager

The Installation Manager provides an easy way of rolling out the different components of FileDirector and to ensure that the components installed on clients are the latest versions.

By creating different profiles, the installation Manager offers the opportunity to adopt the roll-out to different environments. This ensures that on each workstation only the necessary components are installed and provided for further update routines.

Installation Manager Settings on the Server

The Installation Manager is integrated into the server Configuration Utility after its installation.

In the upper part of the Installation Manager tab, the server-installed components are listed. In the lower part of the window, the profiles can be defined and the repository can be updated.

Add Profiles

Default-Profile

After the installation a default profile is provided. If only one profile is needed the settings can be created in this profile.

User Profile

To add additional profiles, select ***Add***, and enter the name of the profile. After creating the profile, it must be branded. After the branding the components for the new profile can be selected.

Within the Setups folder: a branded XML for the Installation Manager.msi for each profile will exist. These will be named ***InstallationManager_profilename***

Update repository

The update repository is under the FileDirector path in the Inetpub folder, and is created after selecting ***Update Repository.*** The default path is:

C:\Inetpub\wwwroot\FileDirector\Updates

IIS Configuration

Anonymous authentication for the update folder must be enabled.

Select the virtual directory of FileDirector and select the subdirectory ***Updates*** and open ***Properties***. The configuration settings of the virtual directory are displayed. Select the tab Directory security.

Edit the option ***Anonymous access and authentication***:

Installation Manager on the Client

Install the Installation Manager with the appropriate profile from the setups Folder. For example, for the ScanUser profile the location to use would be:

http://servername/FileDirector/setups/Installationmanager_ScanUser/setup.exe

For the default profile, use:

http://servername/FileDirector/setups/Installationmanager/setup.exe

Alternatively, the setups can be shared or copied to make them available to the clients.

On the client the Installation Manager runs as the service ***FileDirector InstallationManager***.

If any changes are made in the app.xml of the Installation Manger, the service must be restarted. This can be done by using the two scripts ***ServiceStop.bat*** and ***ServiceStart.bat***.

The App.xml contains the following:

```
<?xml version="1.0"?>
<configuration>
<appSettings>
        <add key="ServerURL" value="http://server01/FileDirector" />
        <add key="UpdateFile" value="Products.xml" />
        <add key="CheckOnStartup" value="True" />
        <add key="CheckTime" value="17:06"/>
        <add key="CheckInterval" value="1" />
        <add key="Trace" value="True" />
</appSettings>
</configuration>
```

CheckOnStartup

True: Checks for updates when the Enterprise Manager or the WinClient is started.

False: Does not check for updates

CheckTime

Once per day on a specified time it is checked for updates.

CheckInterval

This interval is set in minutes.

*The value **0** means no interval.*

Trace

True: A log is created on drive C:.

False: No log is created.

When the Installation Manager updates the software components an update symbol is shown in the taskbar tray.

Upgrade and Update

Software Assurance

The licensing of FileDirector must be within a valid maintenance period to be able to perform an update or upgrade. Please check the expiry date of the maintenance held in the licence. You find the information on the FileDirector server using the Configuration Utility or in Enterprise Manager.

When FileDirector is not within a valid maintenance period, the software assurance needs to be renewed. Contact your authorised reseller. You must import a renewed licence to extend the validity of the maintenance period.

Please refer to the *Licensing* chapter

Notes
Any update to FileDirector, including replacing single DLL's can only be done when the installation is within a valid maintenance period.

Backup data

Web.config

In the web.config from the virtual folder of FileDirector the configuration settings are saved. The old web.config should be saved before an update. During an update the old web.config is updated.

Database

Configuration and all document information is stored in databases. Saving databases can be done using automatic backups executed from scheduled tasks in SQLServer or be performed by physically saving files FD_XXX.mdf and FD_XXX.ldf.

(XXX denotes the unique cabinet ID).

Documents

The document data of cabinets is located in the directory filedirector.data. Below this directory in the subdirectory FD_XXX.CAB is stored (XXX denotes the Cabinet-ID of the relevant cabinet). This data must be backed up.

Upgrade Enterprise Manager and Cabinets

Enterprise Manager has to be uninstalled and reinstalled in order to update; see *Installation of Enterprise Manager*.

Updating of cabinets

After the server test run ***Enterprise Manager***. In order to update a Cabinet, select ***Cabinets*** in Enterprise Manager then choose on the right side of the Enterprise Manager the Cabinets you want to update and use the command ***update cabinets*** from the right mouse menu.

The version numbers should be displayed with the Cabinet name and description.

Upgrade clients

Delete the local cache after an update. The default path is:

C:\documents and settings\USER\My documents\FileDirector.

During a restart of the WinClient the local cache is automatically created.

Plug-ins for WinClient

If you have earlier versions of Plugins installed in the WinClient, they have to be updated to the new versions. The toolbar for plugins can be switched on and off in the menu.

For installation and usage of Plug-ins refer to the User Guide.

Notes
If a PlugIn is not yet available for the current version, please contact your reseller

Transfer special settings of WinClient

To set entries directly for the WinClient, the settings can be configured in the file ***app.xml*** on the client. This file can be found in the program path of the WinClient

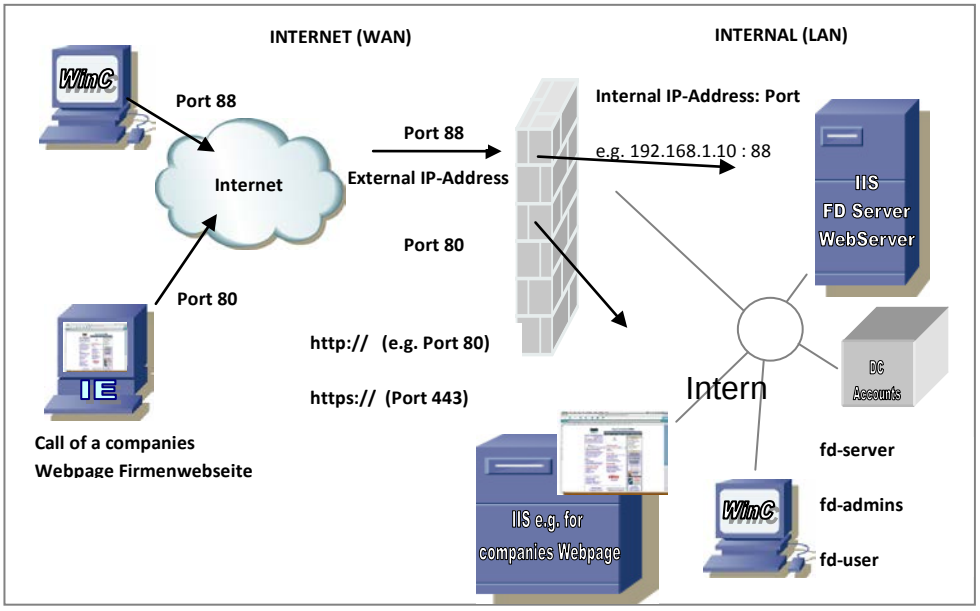
If these settings should be taken over or configured during an update or a new installation, they must be transferred to the server to distribute them with a client rollout.

Migration of ScanFile documents

The migration tool can transfer documents stored within ScanFile to FileDirector. This can be found on the installation CD. Instruction for this tool can be found in the same folder.

Network Security

Usage of different ports

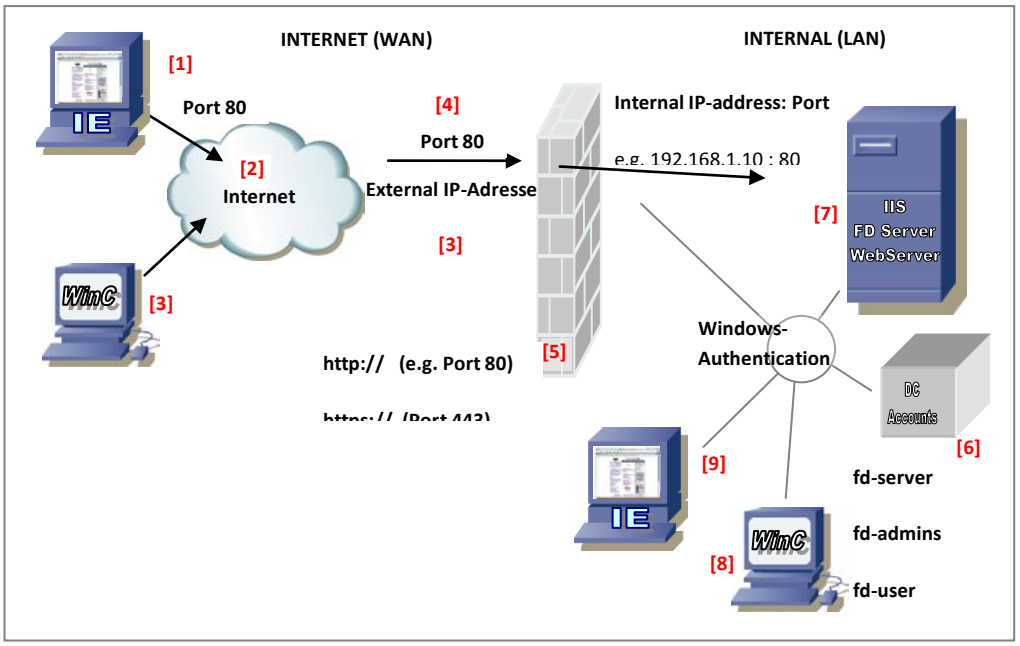


If a request is sent to a server, it is sent to a defined IP address and port (65535 different ports are available). In order to use windows authentication several ports must be open. For a basic authentication only one port is needed.

Port 80 is standard port for this procedure. If a connection via SSL is established, per default port 443 (standard) is used. If several servers in a local network should be called from outside using the same IP address, different ports must be used for each server (example here: port 80 for the companies Webpage and port 88 for FileDirector WebServer). If requests are sent to the external IP address (e.g. 212.17.9.50:88), they are mapped by the firewall to the internal IP addresses.

In the figure displayed above one external IP address with different ports is configured. If port 80 should be used for all applications different external IP addresses can be used. This can be configured using different network adapters.

FileDirector with a firewall



Internal Log-in: Windows-Authentication:

In internal network normally windows authentication is used. This authentication regards all internal windows rights. For the windows authentication several ports are used. If requests come from outside access the system, only one port is normally enabled. Through this port the basic authentication must take place.

External Log-in: Standard-Authentication

An external Log-In is carried out via basic authentication, because only one port is needed and through the firewall only those ports used for communication should be open. The user has to log-in with user name and password on the requested webpage. The user account must be known in LAN.

External Access with log-in using basic authentication:

If a user should access data from the FileDirector sever from outside with log-in, he must be known in the LAN with his account and this account must be in one of the FileDirector groups (fd-scan). (Accounts on domain controller [6])

The user calls FileDirector with WinClient [1] or WebServer [2] via Internet [3] and receives a Login-window.

The Firewall [5] has only one open port (80) [4], which only allows basic authentication. In IIS [7] basic authentication must be allowed.

For log-in of internal clients [8] and [9] Windows-authentication can be used. This must also be activated in IIS on [7].

External access without log-in:

If a user should access data from the FileDirector sever from outside without a log-in or with not having their own account in the network, anonymous authentication can be used. A special windows user for anonymous access is configured. IIS provides a default account ***IUSR_Servername*** for anonymous access.

If ***IUSR_Servername*** must be able to access FileDirector data, the account must be member of one of the FileDirector groups of the domain [6], for example fd-scan.

In IIS [7] anonymous access is allowed for this account in the application FileDirector\Web.

If an unknown user logs to WebServer [7], he should connect with account IUSR. This anonymous user is stored in web.config by ConfigUtility so that WebServer can automatically use it.

The Firewall [5] only offers one open port (80) [4], which only allows basic authentication. Therefore in IIS [7] basic authentication must be allowed for application FileDirector\Web.

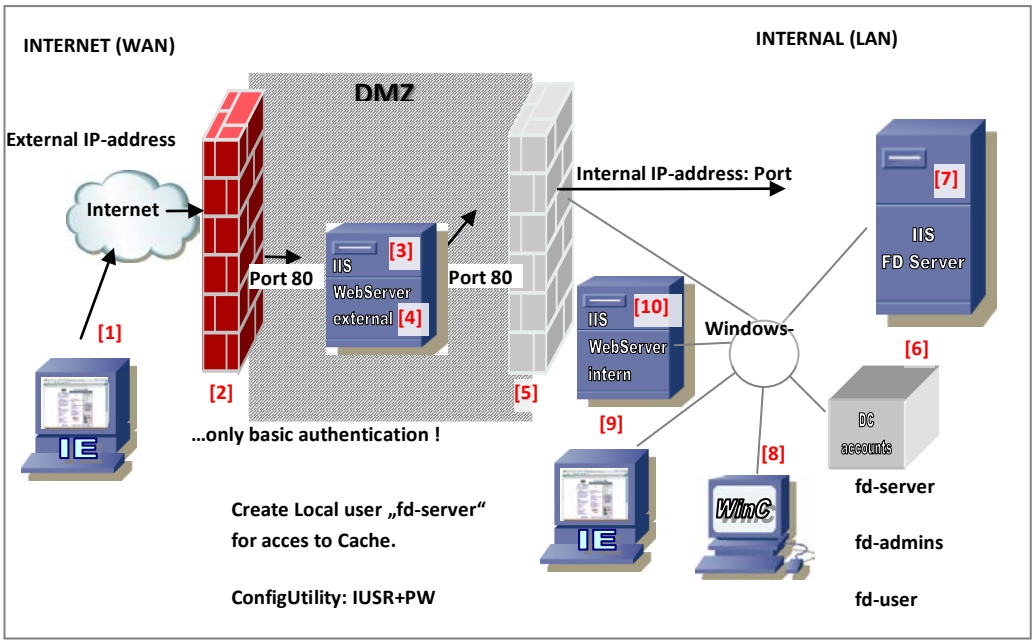
Security problem using WebServer in internal network

If for example a Trojan is infiltrated into a network (by an Email), this Trojan might open ports of its own and establish a connection over different ports. If only one firewall exists, the open ports are directly available for attacks from outside.

In order to avoid that access to the internal network is carried out directly from the internet a demilitarised zone (DMZ) can be setup using a second firewall.

FileDirector WebServer can be configured in this zone. In DMZ only basic authentication with a single port is allowed.

Configuration with a DMZ (Demilitarised Zone)



Login via Internet (WebServer)

User calls WebServer with http://[external IP]/filedirector/web and receives a Login-window.

Firewall has only one open port (80), which allows basic authentication.

In IIS for application 'FileDirector\Web' only basic authentication is allowed. On server [3] a local account 'fd-server' with the same password as on FD-server [on 6] must be created to ensure that that the local cache of the external WebServer [4] can be controlled.

Since a user must log-in with an account known to FileDirector, no account should be specified in WebServer.

Firewall only has one open port (80), which allows only basic authentication.

On domain controller the account logged in must be known and be a member of one of the FD-groups (for example fd-scan).

The account is known to FD-Server because it is member in group fd-scan. In IIS basic authentication must be set, because a user can access the network only by basic authentication.

For log-in of an internal client windows authentication can be used. This must also be activated in IIS [7] for application ***FileDirector***.

For internal usage of WebServer an internal WebServer [10] should be setup. For an internal windows log-in option ***Windows authentication*** can be set in IIS [10] for the application ***FileDirector\Web***. An Internal WebServer can also be installed on the same server as the FileDirector Server [7]

Anonymous Log-in via Internet

A User calls WebServer via ***http:///[externalIP]/filedirector/web*** and receives a login-window.

The Firewall has only one open port (80), which allows basic authentication.

In IIS anonymous access is allowed (IUSR + password). On the server [3] a local account ***fd-server*** must be created in order to control the local cache for WebServer [4].

In WebServer this anonymous account is stored (in file web.config – settings carried out with ConfigUtility). The user is locally created on the machine where the WebServer is installed

Firewall has only one open port (80), which allows basic authentication.

In the domain the same IUSR is created with the same password as on [3]. This account must be member of fd-scan.

FD-Server knows IUSR, because the account is member of group fd-scan. In IIS basic authentication for log-in of IUSR must be activated.

For log-in of internal clients [8] and [9] windows authentication can be used. This must also be activated in IIS on [7].

DMZ settings in Enterprise Manager

During the transfer of data, only specific commands to execute should be allowed.

To allow this in FileDirector the DMZ mode can be activated where just selected commands can be allowed.

The settings can be configured in Enterprise Manager:

System configuration → server → active → select server → properties → DMZ settings

General Administration

Settings in web.config

The file web.config is stored in the virtual directory of FileDirector for general settings. Apart from a few exceptions the keys are set by the FileDirector Configuration Utility. However, additional settings can be set for specific purposes can in the section <appSettings>.

```
<appSettings>
        <add key="WebConfig.Version" value="2" />
        <add key="Server.Language" value="de" />
        <add key="Server.Description" value="FileDirector Web Service" />
        <add key="Server.SessionTimeOut" value="30" />
        <add key="Database.Type" value="MSSQL" />
        <add key="Database.IntAuth" value="True" />
        …
        …
        …
<appSettings>
```

After changes of the web.config a restart of the IIS should be performed. A restart can be done quickly by entering the command ***iisreset*** via ***Start → Run*** on the FileDirector Server. The IIS will be started at the next access e.g. via the WinClient or the Enterprise Manager automatically. This can lead to a short delay when accessing.

Notes
Note that the web.config from versions 1.5 or earlier may not be able to be updated to the latest release. Specific settings may have be copied from the old to the new web.config.

There should be no other file in the server directory that has the extension ****.config*** *so as to ensure the correct configuration file is loaded.*

Configure <identity impersonate="false" />

Change this entry in the web.config to ***false*** if the value is still on ***true*** from a previous version.

If identity ***impersonate="false"*** in the file Web.config is set, the authentication information of the basic processes is used.

This setting is important to avoid problems during the log in.

Stored Domain name

<add key="FDServerDomain" value="Domain name" />

Name of the domain - If the installation should be performed for a domain and the name of a local machine is listed, the ConfigUtility was started with a local log-in.

Number of search results

<add key="SQLMaxDocsInHitlist" value="1000" />

This entry limits the number of search results returned to the WinClient. If a search operation results in more than 1000 entries, only the first 1000 entries are returned to the WinClient. This setting can be changed in the Configuration Utility.

Rename FD-groups

It may be useful to rename the fd-groups.

In the Configuration Utility the groups can be configured and are saved in the following section ***<appSettings>*** of the web.config file:

```
<add key="Accounts.FDAdminsGroup" value="fd-admins" />
<add key="Accounts.FDScanNamedGroup" value="fd-scan-named" />
<add key="Accounts.FDScanConcurrentGroup" value="fd-scan" />
<add key="Accounts.FDUserNamedGroup" value="fd-user-named" />
<add key="Accounts.FDUserConcurrentGroup" value="fd-user" />
```

The value (value=…) for the default group name can be changed. For FileDirector only these groups are relevant. Other groups can be added to these groups to make them known for FileDirector.

Notes
If other groups were used and created in an earlier version, these groups must be mapped. If they are not mapped, they are not included and can be deleted.

Creating documents with 0 pages during index import

If the connection field during the index import is not found in FileDirector it's possible to create documents with 0 pages.

To configure this, in the file web.config the following entry must be set:

```
<add key="FDServer.IndexImportCreate0PageDocs" value = „1“ />
```

Deleting double documents during index import

If documents are imported several times, it is possible that repeated identical documents exist. To delete these double entries from the database and delete them also from the document storeage pool the following key can be set in the web.config:

```
<add key="FDServer.DeleteDuplicateDocuments" value="D:\Pfad\" />
```

Notes
The path must be on the same storage location as the FileDirector server application.
ATTENTION:
The data is moved to the path which is configured and is deleted completely from the FileDirector database and storage pool.

Move index file after index import

If the index import file should not be read after an index import, the file can be moved to a subfolder. This subfolder is automatically created in the index import folder and is named \save. To configure that the file is moved, the following switch can be set in the web.config file of the FileDirector server:

<add key="FDServer.ImportSourceCopyTo" value="1" />

Threshold for signature recognition

When recognising a signature a certain tolerance must be followed. This tolerance can be set in web.config. The lower this value is, the easier a signature can be recognised.

Note, that decreasing this value also decreases security, because a signature can more easily be falsified

To set this threshold, the following value can be changed:

Default value is 80.

<add key="FDServer.SignatureThreshold" value="80" />

Set AND- or OR- relation for field filters

If field filters are used for users or groups there are different conditions necessary for different requirements. With an entry in the web.config this setting can be configured generally to an AND or an OR Relation.

For multiple filters within one field for a user

The following switch is set to value 0 or 1 where:

0 = OR ***1***= AND
<add key="FDServer.FieldFilterSetToAND" value="0" />

For filter in several fields for one user:

0 = AND ***1*** = OR
<add key="FDServer.CombineSearchFieldsWithOR" value="0" />

When the entry is not present ***AND*** is set as the default value between the various fields.

Notes
Please read in addition the section **Relation of AND/OR filters** *in the administration manual.*

Do Not store document info Log

For every document a history is created which can be viewed with the ***Info*** for the document. All actions performed upon the document are logged, - manual changes and automatic changes from the schedulers, e.g. Index-Import. This log is stored in the table ***doclog*** in the database.

An automatic action performed by a scheduler is an action from the user fd-server.

In some circumstances, many schedulers are used for automatic actions that the log becomes extremely large and the size of the database grows. To avoid this, the following switch can be set in the web.config:

```
<add key="FDServer.DisableDocLogLogging" value="0" />
```

With a value of ***0*** all automatic activities of the schedulers are logged. With a value of ***1*** all actions from the fd-server are not written in the table “doclog”.

All manual activities performed by users are still logged.

Notes
This setting only affects the document-Info, not the audit trail accessed from Enterprise Manager. Scheduler activities are still recorded when configured.

Use ODBC connection with password

For an OCBC connection which requires a password, you can set the following entry in the web.config file.

Example1 (Standard setting):

```
<add key="FDServer.ODBCConnectionString"
value="DSN={0};Trusted_Connection=Yes;Connection Timeout=600;" />
```

Example2 (Setting with password):

```
<add key="FDServer.ODBCConnectionString"
value="DSN={0};UID=admin;PWD=password;Connection Timeout=600;" />
```

The term {0} – if available - is replaced in runtime with the ODBC-source, which can be selected in the ODBC-Links.

The setting {0} is not changed manually - ***Trusted_Connection=Yes*** is the previous standard setting used by the fd-server as log-in. If this log-in malfunctions, you can set a user with password by using the key. UID=user, PWD= Password.

Notes
Exception when using external ODBC-driver:
If the ODBC driver set is not windows compliant (In DSN={0}the data source will be loaded from the registry from: HKLM\Software\ODBC\ODBC.ini) the data source cannot be allocated and the connection cannot be established. For this exception you can set the data source for DSN={0} directly, but keep in mind that the result is that only one ODBC-source can be used.

Preserve ODBC Search Result

When using ODBC searches to complete index data, the key below can be set to preserve and use the data found from the previous search, when the current search does not produce a result.

```
<add key="FDServer.UseLegacyODBCResult" value="1" />
```

A value of ***1*** will preserve the results of the previous search. A value of ***0*** will clear the index fields when no results are returned.

Leave user name and last date of changes

When a document is checked in, the user and the date of last changes are saved with the document automatically. If another automatic change by a scheduler or a server plug-in takes place, the changes will be done by the user of the server ***fd-server,*** and the date and the user is updated to ***fd-server***.

If the information should be updated only after manual changes, the following entry can be set in the configuration file web.config:

```
<add key="FDServer.LeaveDocumentModifiedInfo" value="1" />
```

If the value is set to ***1***, the change date and the user are not overwritten with the user ***fd-server***.

Search always with inverted commas (WinClient)

In order that a search in WinClient or in WebServer is always performed with inverted commas, you set the following switch in web.config (“0“ = off, “1“ = on):

```
<add key="FDServer.SetQuotedIndexSearch" value="1" />
```

A search is performed exactly for the string which is entered in the index field, even if a blank is used.

Web Config 2xhash

To improve the security a doubled checking of the hash code can be set up in the file web.config ("0" = off, "1" = on):

```
<add key="FDServer.DoubleHashVerification" value="0" />
```

Relocate local cache when server profiles are used

The WinClient and Enterprise Manager uses a local cache to store new documents, recently displayed documents and settings. This cache is normally located as a subdirectory ***FileDirector*** in the user accounts ***My Documents***.

In some network environments the directory ***My Documents*** is located on a central network storage location in order to include this data in backup strategies.

Because of performance and being able to work offline (without connection to the server or network at all) it is advisable to relocate the local cache to a local directory.

The storage location of local cache can be set in the file APP.XML on the server, which is then copied to the application path of the WinClient and Enterprise Manager. If the path to the local cache is changed after installation and the relevant path entry is not available in the file APP.XML on the server, it can be changed directly in the app.xml of the WinClient and/or Enterprise Manager.

C:\Program Files\Spielberg Solutions GmbH\FileDirector WinClient
C:\Program Files\Spielberg Solutions GmbH\FileDirector Enterprise Manager

```
<appSettings>
<add key="LocalCacheKey" value="Personal" />
<add key=" LocalCachePath" value=" />
</appSettings>
```

Set path in with keys:

The possible values for ***LocalCacheKey*** are

ApplicationData	History	ProgramFiles
CommonApplicationData	InternetCache	Programs
CommonProgramFiles	LocalApplicationData	Recent
Desktop DesktopDirectory	MyComputer	System
Favorites	MyDocuments	
	Personal	

The default value is ***Personal.*** When changing this value to ***ApplicationData*** the cache is created in the following directory:

…Documents and settings\<user name>\Application data

Set path directly:

The key below allows you to configure a path for the local cache directly.

```
<add key=" LocalCachePath" value="C:\LocalCache\FileDirector\" />
```

Component Service with changed local cache directory

If the local cache was replaced on the clients, the local cache directory may only be accessible for the currently logged on Windows user (rights settings). Component service normally starts under the account ***SYSTEM***. If this account is not allowed to access the local cache directory, OCR recognition will fail and generation of thumbnails of electronic documents with the EDOC engine is not possible.

Start Component Service under user Account

The Component service on a client can be configured in services to be started under the relevant user account to ensure access to the local cache directory.

The User account and password must be entered if this user should work with OCR engine.

Switch off Component service

If the following registry entry is set to ***1***, the FileDirector Component Service will control the OCR and EDOC engines. An automatically started Component service is the default setting.

This value is automatically set when Component services are installed on a client PC with Windows 2000 (or later).

```
[HKEY_LOCAL_MACHINE\SOFTWARE\FileDirector\Component Service]
"Installed"=0x00000001 (1)
```

If the local cache location was changed, and only the user account has access to it, the entry ***Installed*** set to ***0*** can also be used to enable the usage of the OCR engine. In this case even on a Windows2000 client (or later) this registry entry must be manually set to ***0***. The ***Component Service*** must be stopped and be set to the startup type ***Manual***. As soon as the OCR is used, the OCR engine will start under the user account currently logged in and will have access to the local cache.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\FileDirector\Component Service]
"Installed"=0x00000000 (0)
```

Using the ImagePrinter with changed local cache

See chapter → *Set pointer to the changed local cache for ImagePrinter*

Move Cabinet to a different FD server

The Cabinet Structure can be exported and imported to create a new Cabinet on the same or a different FileDirector server. Please read the chapter ***Save structure as*** in the Enterprise Manager Manual

Transfer Entire cabinet with Data

To move a cabinet to a different server, the index data and the stored documents of a cabinet have to be copied. To grant access to the documents, accounts and account rights have to be adapted to the new environment.

When a cabinet is moved to a new FileDirector version, the cabinet may have to be updated.

- Copy the database and transaction.log
- Copy the document storage locations (the default is ***filedirector.data***)
- Connect the database in the new SQL server environment
- Register the cabinet in FileDirector Enterprise Manager
- Run cabinet update in Director Enterprise Manager
- If necessary - adjust cabinet rights
- Configure storage pool

Notes on FDConfig:
The database FDConfig stores general configuration information, and also information on all registered Cabinets. The configuration on a different server will be different. It is recommended not to copy the original database but to create a new database FDConfig.

Copy Database

Document index data is stored in the cabinet database. The database consists of the database itself (.mdf) and the transaction log (.ldf). These files are located in the path specified in the Configuration Utility

The 8 character ID of the cabinet is used. In the database directory you will find:

FD_XXXXXXXX.mdf
FD_XXXXXXXX.ldf

Where ***XXXXXXXX*** denotes the ID which is displayed in cabinet properties in FileDirector Enterprise Manager.

Notes
Whilst SQL server accesses the databases the files cannot be copied. The server access must be switched off if these files need to be copied. This can be done by:

a) Stop SQL-server-agent
(This is not recommended during normal working hours, because it stops database activities. No retrieval or storage is possible.)

or

b) Configure a scheduled backup task in SQL server to backup the database. Copy the backup database.

Copy FileDirector.Data

The ***filedirector.data*** directory is the default directory for a storage pool. It contains image and XML data of the documents stored in a cabinet. A

subdirectory is created for each cabinet named with the cabinet ID: FD_XXXXXXXX.CAB

In order to retrieve documents of a moved cabinet in the WinClient the directory with the Cabinet documents must also be copied to storage pool of the target server.

Connect database

Before a cabinet can be registered in FileDirector, the database must be connected within SQL server.

Start SQL server Management Studio on the target server select the SQL group where FileDirector is configured. Right-click on ***Databases*** and select ***all tasks → Connect database***. Select the mdf-file of the database to be connected in the displayed window. The transaction log is automatically selected as well after the mdf file is selected. In this window the authentication method for the database access can be specified. If you use windows authentication no settings have to be made. If you complete these settings, the database will then appear in the list of databases of the SQL server.

Register Cabinet in FileDirector

If the database is connected in the SQL Server it can then be registered to the target FileDirector Server. Open FileDirector Enterprise Manager and right-click on ***Cabinets***. Select properties and the database can then be registered as a Cabinet.

Database Update

If the cabinet was created using an earlier version of FileDirector and is then moved to a newer version, a database update must be performed. This can be done within Cabinet properties.

Configure rights of new cabinet

In the previous environment/network other users might have been assigned to the cabinet or even the administrator might be from a different domain. It is possible that there are no rights on the cabinet even under administrator account of the new environment.

Open the cabinet database in SQL Management Studio and right-click on the table ***Cabrights*** and select ***Edit Top 200 rows*** The Group ***fd-admins*** is displayed. This group was created in the old environment and is listed as ***Domain name\fd-admins***. If necessary rename the domain name to the new domain name. After this change, the administrator account of the new system is accepted for this cabinet.

Notes
Rights cannot be granted directly in the database.
If all records are deleted from the table **CabRights** *in SQL Enterprise Manager, the current user, who must be in the group* **fd-admins** *is automatically added to this list with full rights once a cabinet is reregistered with FileDirector Enterprise Manager.*

Adjust storage pools

In order to display documents in the WinClient, the FileDirector Server must be able to find the stored documents. If the storage pools are configured differently on the new system compared to the old system, the documents will not be found.

Open the cabinet in FileDirector Enterprise Manager and check if the path settings of the storage pools point to the stored data, which were copied to directory \filedirector.data. If this directory is stored on a network device, the account fd-server must have full access.

Proxy server settings

If a proxy server is used in an enterprise, this can be specified in the settings in Internet Explorer.

Open Internet Explorer and select ***Tools → Internet Options → Connections*** then select LAN settings and enter the settings of the proxy server. When a proxy server is used, the settings are displayed here. FileDirector then uses these settings. Under Advanced… addresses can be specified which should bypass the proxy server.

Proxy server with password

If a proxy server with password is used, FileDirector will log on to the proxy server using FileDirector's authentication method – either basic authentication or integrated windows authentication.

Possible manual setting

To avoid a configuration in Internet Explorer, this setting can be deactivated and manual settings can be applied. These settings can be done in the app.xml configuration file of the FileDirector WinClient and the Enterprise Manager.

Enter the following section at the relevant position of the config file, which is located in the relevant program path:

```
<configuration>
  <system.net>
    <defaultProxy>
      <proxy>
        usesystemdefault="true"
        proxyaddress="http://192.168.1.43:8080"
        bypassonlocal="true"
      </proxy>
      <bypasslist>
        <add address="[a-z]+\.domain_name\.com" />
      </bypasslist>
    </defaultProxy>
  </system.net>
</configuration>
```

With the ***setting usesystemdefault="false",*** the system setting of Internet Explorer is ignored and with ***bypassonlocal = "true"*** the setting for ***Bypass proxy server for local addresses*** is configured. Under ***proxyaddress*** the proxy server is specified. In the section ***bypasslis***t a list of addresses can be specified, which can bypass the proxy server.

If the proxy server is bypassed for local addresses, the performance of FileDirector is enhanced, because not all communication must be passed through the proxy server.

Separate Settings in WinClient despite Proxy Settings:

The proxy is bypassed for the WinClient despite the proxy settings for the Internet if the entry below is set in the app.xml of the WinClient.

```
<add key="IgnoreIEProxySettings" value="true" />
```

This option can be set on the server in Setups\WinClient\app.xml for Rollout for all later installed Clients.

Taking over settings during installation

If these settings should be automatically written into the configuration files during the installation of the WinClient or Enterprise Manager, this section must be copied to the file ***APP.XML*** in the installation directory of both applications, with the default path being:

Program Files\Spielberg Solutions GmbH\FileDirector Server\Setups.

Change TCP-port (http: port 80)

By default port 80 is used for FileDirector. If the default port is changed, the port in the IIS settings for the default web page must be changed.

Example: If the TCP-port is set to ***82***, the connection with the WinClient or Enterprise Manager can only be successful if the port in the URL to the server connection is entered.

The server connection to the Enterprise Manager or WinClient must be entered as below:

http://servername:82/filedirector

Notes
The change of a port could be useful for maintenance jobs. You can make sure that no user can login FileDirector if maintenance or an update is being carried out, because the URL with port should be configured at every client.
Once maintenance work is complete, the port can be set back to the old setting.

Information about users and groups

As a basic principle, the group's fd-admins, fd-scan, fd-scan-named, fd-user, and fd-user-named are required.

The group with the FileDirector users must be a member of one of these groups.

To add the users to the cabinet security, the groups must be imported using Enterprise Manager. During this import process the users are written to the table ***accounts*** in the configuration database FDconfig.

A user will be imported at the time when the user logs in to FileDirector for the first time.

Example:

In a company you have the group ***Secretariat***. This group has to have access to data in FileDirector and must have specific rights within the cabinet. To assign these rights add the group to one of the fd-groups (e.g. fd-scan) and import the group fd-scan using Enterprise Manager.

Once that is done, the users and groups are available in Enterprise Manager to set permissions within the cabinet security.

Notes for the server test

Login with password for Windows 2003

If Windows authentication is used, under normal circumstances the login window is not displayed. If the window is displayed Windows authentication has failed and basic authentication is used instead.

If the server is tested with ***http://ipaddress/filedirector*** or with ***http://Server-Name/filedirector*** and, although Windows authentication is used, a login window appears, the server is possibly installed with the windows option ***Internet Explorer Enhanced Security Configuration***

If the server is tested with ***http://localhost/filedirector,*** the login is processed without a password window.

If the enhanced security for Internet Explorer is installed, the browser does not send the user information and Windows authentication cannot be used.

Impersonation Error in: Global.WriteMini

If the message ***Impersonation error*** appears during the server test the login of the user ***fd-server*** was not successful.

Server Audit trail

The login procedure of the FileDirector Server is saved in a log file.called ***fdserver.log,*** and is written in the folder ***Windows\temp\filedirector\server***. The file has a timestamp for every server start.

Here you can possibly find hints to an incorrect start of the server.

Check the password of the fd-server:

Depending on the settings, Windows 2003 Server requires a complex defined password. If, in the ConfigUtility, the user fd-server is created with a password which is not allowed because of the 2003 server complexity rules, the fd-server will have no access to the FileDirector Server.

The password should have a minimum length of 8 characters, and include a capital letter and/or a number. Parts of the user name are not allowed.

Rules of complexity:

- The password must not contain a part or the full account name of the user
- It must have a minimum of 8 characters.
- It must contain characters from three of the four following categories:
- Capital letters from A to Z
- Lower case letters from a to z
- Numeric based on 10 (0 to 9)
- Non-alphanumeric characters (e. g. !, $, #, %)

Deleting user FD-Server and recreate with ConfigUtility

To ensure that the password has been changed, delete the user fd-server that was created and recreate it with the ConfigUtility.

Log in as a domain administrator to delete the account.

Alternatively you can perform the following steps:

1. Open web.config
2. Delete fd-server password
3. Save web.config
4. Start the FileDirector ConfigUtility
5. Type in the password for the fd-server
6. Click OK
7. Run the FileDirector server test
8. Check the FDServer.log in the folder Windows\temp

If there are still errors during the login, you may find hints in this log file.

Check the IIS settings

For the FileDirector virtual directory, anonymous access should be disabled. Please read the chapter on the settings for the IIS.

Check the .NET settings

The .NET settings may not be correct. (Setting: Local system (2003) and respectively the entry in the ***machine.config*** for login as ***system*** instead of ***machine*** was not changed. Please read the chapter for the .NET settings.

Internet Explorer Enhanced Security Configuration

If the option ***Internet Explorer Enhanced security configuration*** is configured in the windows installation, this can cause problems during login. First install FileDirector without this option.

Virtual Network Printer

What is VNP?

VNP is a virtual network printer, which converts print data sent to it into TIFF files and stores them in a defined location. From this directory data can be imported and stored in FileDirector.

For example, accounting software can automatically send the print data during a normal print job to VNP without a user having execute the VNP print.

Any user can print and store documents manually by printing to VNP.

VNP is mostly used for outgoing correspondence. If forms such as invoices or delivery notes are printed and always have the same structure and appearance then they can be recognised and indexed automatically by the FileDirector forms recognition and OCR.

Data is directly processed and stored in electronic form. There is no loss of quality when compared to scanning (scan quality, skewing) and indexing is more accurate.

VNP Installation

VNP (Virtual Network Printer) is a device to create image files by printing to a special printer. These files can later be collected, and then stored and indexed automatically. The image files are stored as TIFF files created from print data.

Setup

For VNP installation, run the VNPSetup.msi which is on the FileDirector CD and follow the installation instructions.

Directories

Choose the path (shared path which can be accessed by the users). The folders ***vnp\archive*** and ***vnp\bin*** are created.

The folder in which data is archived from the VNP must be shared for FileDirector to import the data. The folder must be accessible for the user ***fd-server***.

Ports

During the installation a port ***VNP_001*** is created. The driver for the printer must be connected to this port. The port count is not limited.

Service and process

After installation the service ***VNPManager*** is started.

Printer driver

The VNP printer driver is located in the VNP application path. This printer creates a file *.vtx containing the full text information of the data sent to the printer.

It is possible to use any other printer driver, for example HPLaserjet5. This offers other setting options but it is not able to create the additional full text information.

Installation of VNP printer driver:

Installing the VNP printer is carried out in the same way as for any other printer.

- Select Devices & Printers
- Select Add a Printer
- Local Printer
- Choose existing port ***VNP_001*** (VNP Forwarder)
- Select ***Have disk*** and browse to the VNP printer driver
- Select directory ***VNP\ Driver*** (vnpmpxdll.inf) on the CD

If VNP is to be used from Clients, it must be shared by clicking ***Shared as ….*** A test page should not be printed.

Notes
The configuration of the ports must be done directly on the server, not using remote access.

Configure VNP

During the installation the start menu and a VNP icon is created on the desktop. Using this, the configuration tool is started and you can configure the archive folders and printer mappings.

Licensing

To use the licence of FileDirector the VNP needs a licence file *.fda. This is created if you load the FileDirector licence again using the ConfigUtility.

RIP

The memory for VNP is specified, it is controlled dynamically. This value should be set to 128 MB if large files are printed or higher resolutions are used.

If RIP memory is not sufficient, quality can be reduced, prints may not be complete or may contain stripes.

LPD Configuration

When LPD printing is used, the windows driver is not used. This setting is necessary when printing from UNIX clients.

Start LPD (VNP “listens” on port 515)

LPD is used when different clients send print jobs. With UNIX, communication with a printer is mostly done via port 515.

If a print job should be received via LPD, VNP can be set to be ready to pick up data on this port. In this case a printer will not send data via a PrintPlex port but will use a standard TCP/IP port.

Create TCP/IP port for printing from a client

Setup a printer and create a new printer port for this printer:

- Select Devices & Printers
- Select Add a Printer
- Network printer
- Select the printer using IP address or Host name
- Enter the IP address or the Host name
- Configure the port to use LPR

The byte counter should be enabled, so that VNP does not remain in status ***being spooled.***

If VNP is being tested manually without configuring a printer, a spool file or print file (*.spl or *.prn) can be manually sent directly to that port:

At a command prompt

lpr S [IP-address of server] –P [name of waiting queue] <file name>

Notes
Ensure the port to be used for sending is open. Under certain circumstances this port is closed after installation of a service pack (XP SP2) and has to be opened again.

Port printing

If port printing is used, a TCP/IP port is the protocol is set to RAW. The standard port is 9100.

If port printing is activated in VNP, port 9100 is opened and configured to listen for data.

The different ports cannot be accessed individually using this setting.

> *Notes*
> *Port printing should only be used in exceptional cases as there is no way to control whether a job was processed correctly. If no windows printer drivers can be used, printing with LPR is always preferred!*

Output

TIFF (full colour)

Select this option if you wish VNP to create full colour images

JPG Quality

The JPG quality with which a document is created determines the size of a file. The better the quality, the larger the file. Set the desired JPG quality. 10 is the lowest quality level, 1 the highest.

Configuration of archiving storage

Configuration of the archive path

The print ports which were created during the installation can now be accessed.

By default, printing is directed to the port ***VNP_001***. This port is mapped to the default path ***vnp\archive***. If you define additional ports for additional printers, these can be selected from the list and configured to different paths.

Concurrent printing and archiving

To print at archive documents at the same time, select the ***Print*** option and choose the printer.

Process of the VNP - Archiving

A document is printed to the Virtual Network Printer (VNP01). This is connected to the port VNP_001. For VNP_001, the archive path vnp\archive\tiff1 is configured, where the printed file is saved in a subfolder as .tif - file. In addition to that the *vtx file is generated, which contains the full text.

The second port VNP_002 is configured to print during the archiving to a physical printer.

If the printer is configured, the ports can be mapped to the archive folders to which the data will be saved.

From these folders the data will be imported by FileDirector to the Cabinet.

VNP WebPanel

Via the web panel it's possible to make configuration changes, for example, for different emulations.

Full text with VNP (.vtx - File)

In addition to TIFF files, a .vtx-file is created. This is a file containing full text information derived from the electronic document. It contains the text information of the printed document and is used for full text searching instead of OCR recognition of the TIFF files.

There are no recognition errors because the text information is not collected by an OCR recognition process, but directly from the source data.

This is a big advantage for full text searching in East Asian languages, because the characters are directly copied from the document.

When importing documents, the full text information is automatically stored if a .vtx file is present. OCR recognition is not required.

Portrait and Landscape

The format is automatically recognised, if a document is printed. If e.g. in Word, a document is printed and the tiff file created, is automatically rotated in the VNP archive folder. Then documents can be read in landscape format in FileDirector.

Import of VNP- Data to FileDirector

FileDirector File Import Scheduler

VNP stores the converted print data as TIFF files in a defined archive directory. These documents are ready to be imported into FileDirector. The archive directory must be used as the source directory for a file import scheduler.

Setup OCR forms for VNP

If OCR forms need to be created for documents which are printed with VNP, use a sample print document which was printed from VNP. The method to create forms is described in the Administration Guide.

Setup procedure:

Setup VNP and print a document, which should later be printed and automatically indexed.

Create an OCR form in Enterprise Manager and load the TIFF file from the VNP archive directory created by the sample print.
Configure zones and identifiers for this form.

If the zones are recognised correctly, configure a ***file import scheduler*** using forms recognition to import the documents printed with VNP. See the procedure described in Administration Guide.

Administrative information to VNP

The installation of VNP should be performed directly on the server and not using remote access, because additional print ports cannot be added when using remote access in Windows.

Rights

To the archive folder

To ensure that VNP data from the archive folder can be imported by the FileDirector scheduler, the ***fd-server*** user account must have permissions to this folder. The account must be able to save, delete, move, copy and create folders.

Remove installation of VNP

If VNP is uninstalled the configuration of the port VNP_001 must be reconfigured after a new installation, because this port is automatically created during an installation and in an uninstallation it is automatically deleted.

Restart of the VNP Service

The VNP installs the service ***VNP Manager***. In case VNP needs to be restarted, it can be done via the Windows control panel.

Image Printer

Overview

The Image Printer is a printer driver which converts an electronic document to TIFF files which is then stored automatically to FileDirector. Index information can be applied to the documents prior to storing.

Installation with SetupIP.exe

Installation

If an Image Printer is already installed it must be uninstalled before the installation of the new one. If it has already been printed with the old image Printer, data can be blocked. It is better to restart the machine before the old driver is uninstalled.

The driver can be manually installed as before or the installation can be run using ***FileDirector ImagePrinter Setup.msi***. The installation adds a local port named ***FDPort***. With the FdimagePrinter.inf a printer driver is installed which is connected to the created port.

Operating systems

The printer driver can be installed on 2003, 2008 and 2012 servers and Windows XP, Vista, 7 and 8.

Notes
Resolutions can be set up to 400dpi.
Microsoft support for Windows XP ceases in April 2014. It is recommended that installations still using Windows XP are upgraded to Windows 7 or 8.

Formats

The Image printer supports formats such as A3, A2, A1 and A0 and resolutions up to 600 dpi.

Note that a lot more memory should is required when larger paper sizes and higher resolutions are used. This especially applies to printing with grayscale or colour.

Notes
When possible, colour mode should automatically select black/white mode.
It is possible that black/white pages are converted to grayscale during the print process and a large jpg file is created rather a Tiff.

For this reason you should switch to force S/W mode if large sized formats with colour are printed. Only one coloured pixel is enough and the s/w mode is not used but coloured mode.

Customised paper sizes

To define paper sizes go to printer configuration:

Start → ***Settings*** → ***Printers and Faxes***. In this window all available printers are listed. In the menu ***File*** → ***Server properties*** configurations for the local printers can be set. On the tab ***Forms*** an existing or new customised form with free size can be configured. The maximum size is 137 x 137 cm. After saving the configuration this size can be used by all printer drivers which allow customised formats.

Changed local cache for ImagePrinter

The local cache of the WinClient is by default in ***My documents***. In special cases this local cache is moved to another folder. If you work with the ImagePrinter, this needs to run the Index capture mask the pointer to the Office Link in the local cache.

See section → *Relocate local cache when server profiles are used*

If the cache is moved, the ImagePrinter must also know where it can be found. This is set with an entry in the registry:

Notes
Entries in the registry are only allowed to change by an administrator. Before changing anything in the registry, a backup needs to be created as these are important system settings.

Example:
If the local cache is e.g. in E:\FD_CACHE.

In the entry HKEY_LOCAL_MACHINE - SOFTWARE\FileDirector the new key **Image Printer** *must be created. In this new key a new string value* **redirect** *must be configured which is linked to the folder \OfficeLink.*

Using ImagePrinter

Requirement

The WinClient must be installed on the workstation and the local cache directory for this printer must be present under:

\My documents\FileDirector\Office Link.

The documents printed by Image Printer are initially stored here.

Print and Index

Start the WinClient.

Open, for example Word, create a document and print it with Image Printer. The ImagePrinter index capture window appears:

Split documents

Using this function it is possible to split up multipage documents.

After selecting the split document button the multipage document is split into an equivalent number of single-page documents. For each of these new single-page documents created, a new capture window opens once the previous one is closed. This provides the option to index each page individually.

The resulting single-page files are put onto the local list of WinClient.

The index fields can be completed.

Selecting ***OK*** will store the documents in the local list of the user.

In this list the document can further be edited, changed and finally be checked in.

If several documents are printed with image printer the index can be transferred to all documents.

As an example, several delivery notes are printed with the Image Printer and a common field could be filled and selecting ***Apply to all***, the documents can be sent to the local list and the empty fields can be filled.

FileDirector SharePoint Integration

The FileDirector SharePoint Connecter will add the ***Send to FileDirector*** function in SharePoint. In addition, the FileDirector Web Parts ***Web viewer***, ***Full text search, Data view*** and ***Document Upload Manager*** are integrated into SharePoint

Requirements

The SharePoint Connector can be installed on a system with the following components:

- .NET Framework 2.0
- SharePoint Server 2007 or 2010
- FileDirector Component Service

In addition, a FileDirector Server is needed. To create a document link in SharePoint or to use the FileDirector Web Parts, FileDirector WebServer is required. Both servers do not have to be installed on the same system.

Installation

After starting the Connector setup the URL of the SharePoint server is displayed. If necessary, the address can be corrected. Then you can select the language in which the Web Parts are installed. Then the application directory of the FileDirector SharePoint Connector is displayed and can be changed. During the installation process a command window displays the progress of the FileDirector Web Part installation and integration into SharePoint. This installation sequence can take some time.

After a default installation, the FileDirector SharePoint Connector can be located here: ***C:\Program files\Spielberg Solutions GmbH\FileDirector SharePoint Integration***. A menu entry ***SharePoint Connector*** is placed in ***Start -> Programs -> FileDirector***, and an icon is created on the desktop.

Notes
The Connector will only be available when logged in using the same account used for the installation.

FileDirector SharePoint Connector

The FileDirector SharePoint Connector is used to configure the ***Send to FileDirector*** functionality. The program has no influence on the FileDirector Web Parts.

Open ***Start -> Programs -> FileDirector*** and start the ***SharePoint Connector.*** Select the ***Connection*** tab first. You can enter the addresses of the ***FileDirector Server and WebServer***.

Notes
You cannot configure a connection between SharePoint document lists and FileDirector Cabinets and document types without a connection to the FileDirector Server.

Enter a FileDirector Server address at ***Server URL***.

Select ***Automatically log-in using current Windows account*** when the Windows account of a SharePoint user is to be used for authentication. If this option is not selected, a log-on to the FileDirector Server is required for configuration. In addition, a log-on will be required for each send process later on.

The language used can be adjusted. Select a ***Language*** from the drop down list. The new language is applied after a program restart.

If you want to replace sent documents with a document link in SharePoint, you can add a ***WebServer URL***. This is optional.

Using ***Test connection*** you can test whether the Windows user is a valid FileDirector user and has access to the FileDirector Server.

Now select the ***Settings tab.*** Here you set up the connections between SharePoint document lists and FileDirector Cabinets and document types.

First enter the ***SharePoint Server URL*** and click ***Retrieve***. All available document lists on the SharePoint Server and their addresses are then displayed.

Select all and ***Toggle selection*** relate to the selection of list items. With ***End***, all changes are saved and the program is closed. With ***OK*** you continue to the detailed connection settings for the selected SharePoint document lists.

Select all SharePoint document lists from which documents will be sent to FileDirector and click ***OK***. The next screen allows you to connect SharePoint document lists to a Cabinet and Document Type.

Select a FileDirector Cabinet. The list of corresponding document types is shown. Choose a document type and all visible fields of the SharePoint document list are displayed. Alongside them are the fields of the selected Document Type. When you connect two fields, the contents of the SharePoint field will be written into the matching FileDirector field during the Send to FileDirector process.

Notes
Ensure that the field types of SharePoint and the FileDirector index fields match. Otherwise the FileDirector server will reject the sent document.

SharePoint document lists do not contain any keywords. Nevertheless you can connect a virtual SharePoint keyword list to a FileDirector index field with keyword list. If a document is sent from a folder or an entire folder is sent to FileDirector, keywords are created from the folder and subfolder name(s). Missing keywords are added to the keyword list in FileDirector.

If ***Replace SharePoint file*** is selected, the sent SharePoint files are replaced by a link to the document stored in FileDirector. You have to enter a FileDirector WebServer address in order to create a valid document link. If the option unselected or the FileDirector WebServer address is missing, the sent SharePoint files remain unchanged.

Notes
The document link encloses the FileDirector WebServer address. If the address is changed, the FileDirector document can no longer be displayed using this link. An address is changed by a new FileDirector WebServer address, when the document type of the document is changed or when the identifier of the document is renewed.

Use ***Previous*** and ***Next*** to browse through the selected SharePoint document lists. ***Apply to all*** will copy the current settings to all following SharePoint document lists. If only one list has been selected, these buttons are disabled.

Notes
SharePoint document lists can contain a different number of fields. Using **Apply to all** *can lead to unwanted field connections.*

OK will return to the SharePoint document list display. ***End*** saves all settings and exits the program.

Send to FileDirector

For each SharePoint document list connected with a FileDirector document type, you have to activate the ***Send to FileDirector*** menu entry in SharePoint. Browse to the corresponding SharePoint web page and follow ***Site Actions -> Site Settings -> Modify All Site Settings -> Site Collection Administration -> Site Collection Features***.

The displayed list contains an entry ***Send to FileDirector***. By activating the feature, the entry ***Send to FileDirector*** is added to the context menu of the document list.

Execute ***Send to FileDirector*** on a file and a FileDirector document is created from the file and its index information and sent to the FileDirector Server.

If a folder is sent to FileDirector, each file in the folder is sent as a single document. Files of existing sub folders are processed as well.

The transfer result (success or error message) will be displayed in SharePoint.

FileDirector Web Parts

You can easily access FileDirector documents using FileDirector Web parts without having to install additional client software or to open a second web browser.

Add Web Parts

Browse to the SharePoint web page to which you want to add a FileDirector Web Part. Select ***Site Action -> Edit Page***.

All available Web Part zones are displayed. Select ***Add a Web Part*** to integrate a Web Part into a zone.

A list with available Web Part zones is displayed. The FileDirector Web Parts are listed in ***Miscellaneous***. Select the FileDirector Web Part and click ***Add***.

Notes
*If the FileDirector Web Parts are not listed under Miscellaneous, you need to update the Web Part catalogue manually. Go to **Site Actions -> Site Settings -> All Site Settings -> Galleries -> Web Parts -> New**. Select the FileDirector Web Parts and click on **Fill Catalog**. The Web Parts are now available in the Web Part catalogue.*

If the Web Part is not placed correctly, you can move it with the mouse. Enter all necessary Web Part settings and publish the SharePoint web page.

Notes
Without further adjustments, the Web Part will adjust to the Web Part zone size. Since the display of documents needs a certain amount of space, please adjust the size of the Web Part sufficiently.

FileDirector Web Viewer

The File Director Web Viewer allows users to search and display FileDirector documents.

The message ***No search result available*** is displayed when no FileDirector WebServer address has been entered. To do so, select ***Edit Web Part***. The settings section of the Web Part opens on the right hand side.

The WebServer address (*http://myserver/filedirector/web/SharePoint*) is mandatory. As soon as a valid FileDirector WebServer address has been entered, the Web Part will display the search page of the FileDirector WebServer.

The Web Part settings ***Cabinet ID*** and ***Document type ID*** preselect a Cabinet and document type. Both values are optional.

FileDirector Full text search and Data view

The full text search will generate a search request and forwards it to the FileDirector WebServer. The result is displayed in the FileDirector data view.

Two Web Parts are needed: ***FileDirector fulltext search*** and ***FileDirector Data view***. These Web Parts have to be placed on the same web page, but not in the same Web Part zone.

To prepare both Web Parts for interaction, a connection has to be established. Select ***Edit -> Connections -> Send FieldProvider to -> FileDirector DataView***.

Notes
*If the connection is missing, the data view displays following error: **The FD Dataviewer is not connected with a FD fulltext search Web Part**.*

After connecting, configure the settings of the FileDirector full text search Web Part. Select ***Edit -> Edit Web Part***. The settings section of the Web Part opens on the right hand side. You need to enter the FileDirector WebServer address (*http://myserver/filedirector/web/SharePoint*), a Cabinet identifier and the identifier of the document type you want to search in. This Web Part doesn't change its size, an adjustment is not necessary.

The FileDirector Data View has no FileDirector related settings. All information is retrieved through the Web Part connection. Since the display of documents needs a certain amount of space, please adjust the size of the Web Part sufficiently.

The message ***No search result available*** displayed in the FileDirector Data View means, that the Web Part is connected, but no search has been executed yet.

Notes
From FileDirector WebServer version 2.6 on the full text search web part is obsolete. FileDirector Web viewer displays a search page that already includes a full text search. WebServer still supports these Web Parts.

FileDirector File-Upload

This Web Part is able to send files to the FileDirector WebServer. A FileDirector document is created, which can then be indexed and checked-in.

After the Web Part has been placed into a zone, it needs to be configured. The message ***No search result available*** is displayed when no FileDirector WebServer address has been entered. To do so, select ***Edit – Edit Web Part***. The settings section of the Web Part opens on the right hand side. Enter the FileDirector WebServer address (*http://myserver/filedirector/web/SharePoint*). As soon as a valid address has been entered and saved, the file upload page is displayed in the Web Part. Since the display of documents needs a certain amount of space, please adjust the size of the Web Part sufficiently.

FileDirector Synchroniser

The FileDirector Synchroniser keeps documents in SharePoint lists and FileDirector document types at the same information level.

Requirements

The Setup can be installed on a system with following components:

- .NET Framework 2.0 SP 2
- SharePoint Server 2007 or 2010
- FileDirector Component Service

Additionally, access to a FileDirector Server is needed. The server does not have to be installed on the same system.

Installation

The setup will install all programs without user interaction.

After the installation a menu entry ***SharePoint Synchroniser*** will have been created in ***Start -> Programs -> FileDirector***.

The Synchroniser Engine is installed into the directory ***C:\Program Files\Spielberg Solutioons GmbH\FileDirector Component Service\Synchroniser Engine.***

Synchroniser Engine

FileDirector Component Service needs to be restarted after the Synchroniser installation to start and monitor the Synchroniser Engine. Valid program settings can only be configured when the Synchroniser Engine is started.

The Synchroniser Engine will log on using ***Local System*** account.

Any errors that occur will be written into the Application section of the Event Viewer.

Synchroniser

The FileDirector Synchroniser is used to configure the synchronisation process.

Go to ***Start – Programs – FileDirector*** and start the ***SharePoint Synchroniser***.

Before configuring the Synchroniser, you have to create two fields. They are mandatory for the synchronisation process.

Add a numeric index field to every FileDirector document type that is to be synchronised. The SharePoint documents numeric identifier will be stored in that field.

Add a text index field to every synchronised SharePoint document list. Revision data of the connected SharePoint and FileDirector documents will be stored in the field.

Note
Both fields must not be editable by users.

For the best performance select

- SharePoint 2007: ***Documents -> Settings -> Document Library Settings -> Versioning Settings***.
- SharePoint 2010: menu ***Library Tools -> Library -> Library Settings -> Versioning settings.***

Browse to the section ***Require Check Out***. Switch the option ***Require documents to be checked out before they can be edited*** to ***Yes***. If this option is set to ***No***, the Synchroniser will temporarily change this option during the synchronisation process.

Start the FileDirector Synchroniser.

Notes
If the following message is displayed: ***Unable to connect to Synchroniser Engine. Please check your installation.*** *The Synchroniser Engine hasn't been started. In this case restart the FileDirector Component Service.*

Select ***Connection*** tab. Here you can enter the connection to the FileDirector Server and set the synchronisation interval.

Notes:
SharePoint document lists and FileDirector document types cannot be linked without a valid FileDirector Server connection.

Enter a FileDirector Server address at ***Server URL***.

The language used can be adjusted. Select a ***Language*** from the drop down list. The new language is applied after a program restart.

With ***Test connection*** you can specify a user name and password. These credentials are used to log-on to the FileDirector Server and SharePoint Server. Do not use an internal FileDirector account, since the SharePoint Server will not accept it.

Notes
On the FileDirector side the user needs sufficient rights to create, edit, delete and, check-out documents. On the SharePoint side the user needs rights to:
retrieve document lists
create, edit, delete and check-out documents
create, edit and delete in the database of the SharePoint SQL server

With ***Scheduler interval*** you set up the timing of the Synchroniser Engine and its update frequency.

Select the ***Settings*** tab. There you can set up the connection between SharePoint document lists and FileDirector Cabinets and document types.

First enter the ***SharePoint Server URL*** and click ***Retrieve***. All available document lists on the SharePoint Server and their addresses are displayed.

Select all and ***Toggle selection*** relate to the selection of list items. With ***End*** all changes are saved and the program is closed. With ***OK*** you continue to the detailed connection settings for SharePoint document lists.

Select all SharePoint documents to synchronise and click ***Edit***. The next screen allows you to connect SharePoint document lists to a Cabinet and document type.

The current SharePoint document list name is displayed in the ***SharePoint*** section. You have to select two fields.

Select the index field from the document list to store the revision data for ***Connect Field***.

Notes
Without this connection the synchronisation process will fail.

For ***Date field*** select the ***Create*** or ***Change*** date of a document. This date will only be evaluated when the data to be synchronised indicates that a document has been changed in FileDirector as well as in SharePoint. In this case the date field will decide which document is used and which document is overwritten.

Then select a FileDirector Cabinet. The list of corresponding document types will be shown. Choose a document type.

Notes
A FileDirector document type and a SharePoint document list must be uniquely connected. Each synchronised SharePoint document list has to be connected to a different FileDirector document type otherwise the relation is not retraceable.

All visible fields of the SharePoint document list are displayed. Next to them are all document type fields available.

(Connect Field) is used to identify the connected SharePoint document. Select the FileDirector index field where the SharePoint documents identifier is stored in.

Notes
Without this connection the synchronising process will fail.

If you connect two fields, the corresponding index field contents of the target document will be updated.

Folders and sub folders in SharePoint document lists are ignored. Their documents are treated as normal list documents and are synchronized. The folder structure itself is not used in any way.

If documents are to be excluded from the synchronising process, go to ***Synchronising condition*** and select an index field in SharePoint and FileDirector. Add text into the field alongside. If the entered text is found in both index fields, the document is excluded from synchronisation. If the index fields are selected, but no text has been entered, all documents will be synchronised.

Use ***Previous*** and ***Next*** to browse through the selected SharePoint document lists. If only one document list has been selected only, these buttons are disabled.

OK will save all settings, ***Cancel*** discards all settings. Both buttons return to the SharePoint document list display.