DocuWare

White Paper Security

DocuWare

Contents

This document was created using AuthorIT™, Total Document Creation (http://www.author-it.com).

Disclaimer

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by DocuWare GmbH. DocuWare GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

DocuWare GmbH
Planegger Straße 1
D-82110 Germering
www.docuware.com

1 Objectives of this White Paper

This white paper describes the security safeguards within DocuWare software. You will learn which technologies and methods can be used to achieve the main security objectives, as described, amongst others, in the guideline IT Security Guidelines of the Federal Office for Information Security Germany.

These objectives include:

- Confidentiality: documents and data are only accessible to authorized users
- Integrity: documents and data cannot be changed without authorization, changes can be traced
- Availability: DocuWare services and documents are always available
- Access security to the DocuWare system
- Backup of data stored in DocuWare

The security safeguards described refer to documents and data stored in DocuWare.

This white paper does not deal with setting up a DocuWare system, embedding DocuWare in the company's IT infrastructure, backing up databases and file systems outside DocuWare, protecting local computers or DocuWare as a service provider (DocuWare Cloud).

The aim of the White Paper is to enable you to form a technologically well-founded opinion about the security of DocuWare on-premises system.

The paper is aimed at readers with an interest in technology, particularly technical staff at clients, sales partners, and consulting firms, as well as specialist media. It assumes a certain level of technical knowledge about the structure of modern software applications, ideally of document management systems.

2 Introduction

DocuWare is the modern solution for document management and workflow automation. DocuWare lets you access documents and important information they contain at any time and anyplace.

The documents are stored centrally in file cabinets. Documents can be viewed and edited in the browser-based DocuWare Client. It is also possible to load documents from DocuWare into the file system.

Thanks to the numerous indexing functions, all document types are always stored in the right place and brought back to the screen with just a few clicks.

These and many other functions, such as workflow management, make DocuWare a powerful software that allows you to optimize your business processes. The DocuWare website also provides information on the various fields of application.

DocuWare's security concept follows the principles of the General Data Protection Regulation (GPDR), which require the protection of personal data through technical design and data protection settings.

If you would like to know more about the technical aspects of DocuWare, visit the DocuWare Knowledge Center and the DocuWare website:

- White Paper System Architecture
- White Paper Integration
- White Paper Intelligent Indexing
- White Paper DocuWare Cloud
- Compliance and Certificates

3 Access security

Access to the DocuWare system and the file cabients is protected by a login procedure and by secure data exchange between the components.

Authentication checks and verifies the identity of the user who logs on. This also applies to IT components or applications that are to access the DocuWare system.

More information on the design of DocuWare in the White Paper System Architecture.

3.1 Login Methods

The login to DocuWare is always verified via Authentication Server. Authentication Server manages all users, licenses, resources and rights of a DocuWare system.

The login procedure also incorporates a verification of the licenses available to the user. The following user authentication methods are supported by Authentication Server:

- **DocuWare Login**
  Users must prove their authorization by means of the name and password as stored in DocuWare.
- **Trusted Login (Single Sign-On)**
  The client is identified without any other user input by using the credentials of the current Windows operating system session. Authentication Server verifies these credentials directly. Trusted login can only be used if client and server are located in the same Windows domain network.
- **Login Token**
  Tokens are an internal logon mechanism which is mainly used for Single Sign-On between different DocuWare components. For this purpose, the Authentication server issues tokens to an already authenticated user in application A. The token is then passed in a secure way to application B which can in turn use the token to authenticate with Authentication Server. So the user has, for example, not to log in again, if he uses first Web Client and then DocuWare Configuration.

Most DocuWare components communicate via HTTP(S). Once verified, credentials are sent in encrypted form from the server to the client, which uses this string to authenticate subsequent requests. The user is verified automatically for example when the browser is reopened.

3.2 Passwords

In addition to the passwords of DocuWare users, the database server password and the password for the mail server are cryptographically stored securely so that only the server components can decrypt them. This is to keep them secure, even if you have users that have access to the database such as backup operators.

Technical implementation

The PBKDF2 algorithm (Password-Based Key Derivation Function 2) is used for password encryption. A hash function is applied to the password together with a salt value. The combination with a random value does not produce the same hash value even with two identical passwords. The function is then applied to the result several thousand times. This procedure makes it difficult for hackers to deduce the original password from the hashed value using brute force attacks.

Password Settings

The complexity of passwords within the organization can be specified in DocuWare Administration. For example, passwords must then have at least one capital letter, one lower-case letter, one number and/or one special character. In addition, you can define the minimum length of the password, how many days it remains valid and how many incorrect entries are possible before the user account is locked.

The administrator of the organisation can disable the password time limit again for specific users. This is particularly useful when services need to log on to a server as users.

If a user should forget his password, he can demand a new, automatically generated password sent by email via a link in the login dialog of the Web Client. The user can use this to log on to Web Client and set up a new personal password.

Alternatively the organization administrator can reset the password. However, this is not possible for high-security-users. These users have to restore their password for themselves (also see the chapter High Security System (on page 16)).

3.3 Communication between Components

To prevent an external attack and the unauthorized access of data, it is important to **secure the communication between the web-based client applications and the platform service with SSL/TLS (HTTPS)**.

To configure the DocuWare Web components for HTTPS (SSL/TLS), you must carry out the following steps in IIS manager:

- Import the certificate or certificates ("server certificate", "Import" action)
- Adapt the website binding and make it accessible via SSL/TLS
- If necessary, remove the HTTP binding for security reasons (optional)

4 Authenticity of Documents

Data is considered authentic if it can be assigned to its origin at any time. In DocuWare, the origin of stored documents can be verified by means of unchangeable system entries and electronic signatures.

4.1 System Entries of Documents

When a document is stored in DocuWare, system entries are automatically created that cannot be changed by users in DocuWare. The following system entries for the user, date, and document changes and accesses provide information about the origin of the document:

- Store User
- Store Date
- Modification Date
- Modification User
- Last Access Date
- Last Access User
- Document ID

You can access system entries from the context menu of a document in the result list: *Edit Index Entries > System Entries*.

4.2 Electronic Signatures

An electronic signature serves the same purpose as a handwritten signature for paper documents. It largely ensures that a document really does originate from the author. Signatures can also be used to verify and verify changes to documents.

A document is already digitally signed with an indication of the author or sender, whereby a simple signature is not subject to any special provisions for protection against forgery. A scanned signature inserted in DocuWare by stamp can act as a simple electronic signature.

To clearly identify yourself as the author of a document, you can select a certificate for a document in PDF-A format when importing it into DocuWare. The certificate must be in the Windows certificate store on the client machine and only the user can access it.

Certificates should have the following characteristics:

- RSA Certificate (recommended)
- Length: 1024 bit minimum, 2048 bit recommended
- Key application: digital signature

A document imported with a certificate can be stamped and annotated in DocuWare, but cannot be edited.

5 Confidentiality: Document Access for Authorized Users Only

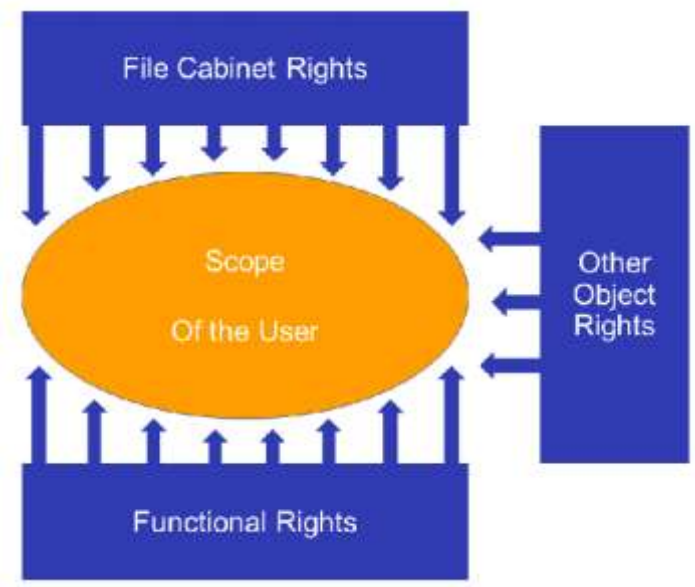
Employees in large organizations deal with complex processes and are subject to a variety of rules and regulations. In order to carry out their tasks they need authorization to use particular resources such as document and IT functions.

However, restrictions are also necessary to achieve the security objective of confidentiality. Certain restrictions make sure that only authorized personnel have the right to do certain things, and maintain transparency for everyone.

DocuWare uses a rights concept which allows you to define in great detail, for each DocuWare user, which activities he or she can perform within the DocuWare system.

5.1 Rights

The distinction between functional rights and file cabinet rights is essential for rights administration in DocuWare.



Thanks to a complex rights-structure, the user's activity scope can be determined in detail

5.1.1 Functional Rights

Functional rights are used to determine which menu items are available to a DocuWare user in the Web Client, in the DocuWare Configuration and Workflow Manager. This includes, for example, the right to create a stamp or a configuration for document trays. The assignment of individual menu functions as rights allows you to define precisely which functionalities are available to a user within the DocuWare system or not. For example, if an employee is not allowed to manage document trays, the module will not be displayed when the user calls up the DocuWare Configuration.

The functional rights are assigned in the DocuWare Configuration in the section *User Management*.

Functional Rights in an Organization

- Edit Select Lists
- User Synchronization
- User Management
- Usage of lists, result lists, search dialogs, store dialogs or folder structures
- Configuration of: auditing, Autoindex, Connect to Mail, Connect to MFP, Connect to Outlook, deletion policies, document processing, document trays, field masks, file cabinets, forms, Intelligent Indexing, notifications, Requests, select lists, Smart Connect, synchronization, text recognition, transfer
- Use SQL commands
- Stamps

5.1.2 File Cabinet Rights

File cabinet rights refer to a file cabinet and the documents stored in it, such as storing and searching a document, editing index entries or exporting documents or a file cabinet to the file directory. Different file cabinets rights can be assigned for different file cabinets.

File cabinet rights are divided into administrative, general and overlay rights as well as field rights.

- **Administrative Rights** include managing permissions, managing dialogs or migrating documents in the file cabinet.
- **General Rights** include storing, searching, and deleting documents.
- **Overlay Rights** apply to stamps, annotations, and graphical elements.
- **Field Rights** include the rights to search, to edit field contents, and to enter values that do not exist in a select list. You can assign field rights for all fields in a file cabinet or for specific fields.

The file cabinet rights are assigned in the file cabinet area of the DocuWare Configuration.

5.1.3 User and Administrator Rights

For a number of other objects, users and roles can be granted "usage" and "admin" rights. The object can be used with the user right, the administrator right contains the right to edit the object or the corresponding configuration.

In order for a user to assign user and administrator rights to an object, this user must first be assigned the functional right for the object, such as the management of document trays. The corresponding module is then displayed in the DocuWare Configuration when the user logs on.

Objects wich can be assinged as user or/and administrator:

- *File Cabinets*
- *Autoindex jobs*
- *Document Trays*
- *Configuration of Document Processing*
- *Notification*
- *Configuration for emails from Outlook*
- *Configuration for emails generally*
- *Forms*
- *Intelligent Indexing*
- *Deletion Policies*
- *Mail Connection*
- *Configuration for a Multifunction Peripheral*
- *Request*
- *Synchronization and Mirror*
- *Configuration of Smart Connect*
- *Configuration of Text Recognition*
- *Transfer jobs*

5.2 Assigning Rights

The rights described in the previous chapter can be conveniently assigned to users with profiles, roles and groups - especially in companies with many employees.

Groups (as sets of users) and roles (as sets of rights) are different ways of looking at one and the same thing. From one perspective, the employees are the starting point. From the other, the starting point is the workflows and functions in the DocuWare system.

5.2.1 Profiles and Roles

Profiles and roles enable you to assign sets of rights in "containers," instead of a lot of individual rights. The assignment of rights to profiles and roles has two advantages:

First, detailed sets of rights can be assigned at the touch of a button to as many users as required, without the administrator having to customize the rights structure manually for each user.

Second, sets of rights also exist without users, so when an employee leaves the company, their successor can be effortlessly assigned the same rights, regardless of how specific the rights assignment is.

- **Profiles**
  Functional rights can be combined to functional profiles, file cabinet rights to file cabinet profiles. Both can be assigned to individual users and roles.
  File cabinet rights are always combined into profiles, meaning, they cannot be assigned directly to individual users. Only file cabinet profiles can be assigned to users or roles. As with functional rights, file cabinet profiles are additive. If several profiles of a file cabinet are assigned to a user, this user receives all the rights that are shared by these profiles. This procedure is explained in more detail in section Interaction of Rights and Permissions.
- **Roles**
  Roles are sets of several profiles. A role can include both profiles with functional rights and profiles with file cabinet rights. Roles can be assigned to groups and to individual users.

5.2.2 Predefined Roles and Profiles

For a quick start with DocuWare predefined roles with predefined profiles are available after a system installation. This means that administrative tasks are also subject to the authorization concept. These predefined roles can be assigned to different users or user groups.

System Administrator

The system administrator manages the system with regard to the hardware and the basic components which are generally needed. The system administrator can be defined so that he or she cannot access individual organizational data, and specifically cannot intervene in the details of the user administration. However, only he/she can assign the "System Administrator" role to other users. This cannot be done within the organization's user administration. It is only possible in the system section of DocuWare Administration.

After DocuWare has been installed, he/she assumes the role of organization administrator for all organizations simultaneously. As each new organization is created, the system administrator initially automatically assumes the role of organization administrator. This can then be assigned to another person.

Tasks of a system administrator

- Providing and maintenance of hardware, operating system and databases
- Installing of the DocuWare Server Modules
- Configuration of system-wide settings for servers, connections for databases and file directories, storage systems and user directories
- Insight into auditing at system level

Organization Administrator

A DocuWare system can include one or more organizations, each with its own organization administrator. The organization administrator manages the rights, users and user groups of their organization. The role does not include access rights to file cabinets and their administration.

This role does not require any detailed technical knowledge of the IT environment. The organization administrator can also assign or remove the role to and from other users. In particular, the role can even be removed from a system administrator.

Tasks of an organization administrator

- Assignment of the licenses
- Creating of users and groups
- Configuration of clients, viewer and document trays, stamps and signatures, select lists
- Insight into auditing at organization level

Default File Cabinet Rights

After DocuWare has been installed, four file cabinet profiles are predefined that can be assigned to users and groups:

- Owner
- Edit
- Read
- Delete

In addition, you can create your own user-defined profiles in the file cabinet settings.

Details on the file cabinet rights

5.2.3 Users and Groups

DocuWare users can be combined into different groups. A user can be a member of more than one group.

- **User**
  As a rule, one user is created for each staff member who needs to work with DocuWare. Users receive a range of rights through the assignment of individual rights or sets of rights in the form of profiles and roles. Users can belong to groups.
- **Groups**
  Groups are sets of users. It is a good idea to combine users into groups which need to use the same program functionalities and be assigned the same file cabinet rights. Individual users receive these rights through their membership of the group, to which the appropriate role has been assigned.

5.2.4 Inherited Rights and Explicit Rights

When assigning rights to users, DocuWare distinguishes between inherited rights and explicit rights.

- **Inherited Right**
  Rights that a user has received through membership of a group or through a role or a profile are called inherited rights.
- **Explicit Right**
  Rights which a user receives directly (and not via a role, profile, or group), are explicit rights. Only functional rights can be assigned as explicit rights.

Rights are always additive, in other words, the total of all a DocuWare user's assigned rights constitute this user's activity scope.

5.2.5 Interaction of Rights and Permissions

If a user is a member of several groups, he or she has all the rights that are available through assignment to these groups and their roles. If several roles or profiles are assigned to a user, this user has all the rights that have been assigned to these roles or profiles.

Examples:

- A user has received his set of rights via a role. If you now assign this user an additional role that has fewer rights, it does not change anything for that user, since rights are additive. In order to restrict his rights, you would have to remove the original role from him. The same applies to groups.
- A user is a member of two groups and has received his set of rights via the roles of these groups. If you now remove the membership of one group from him, he does not automatically lose all the rights that are assigned to him via the roles of this group, but only those that are not assigned via the other group.

The scope a user has in a file cabinet result from the file cabinet rights and access to the dialogs.

Example:

- Two users have a result list which provides the *Download a PDF with annotations* button in its toolbar. One user has the Export-file cabinet right and can make use of this option. The other has not been given this right. The *Download a PDF with annotations* button is greyed out then and the user cannot make use of it.

The settings for the individual file cabinet fields and assigned file cabinet rights overlap in some areas. It is therefore possible to make special rights available to designated users, while "normal" user rights are controlled by means of field settings.

Example:

- A file cabinet field has been specified as a Fixed value in the Store dialog, and a user has the right to modify index entries. This user is authorized to change the fixed field entry in the store dialog and/or in the index dialog of the result list.

Summary: a user's file cabinet rights always override the field rights. Using a combination of both schemes should therefore be done with care.

5.2.6 Restricting Document Access Using Index Data

You can use index value profiles to assign rights according to index entries within a file cabinet. The limitation of document access via index data is particularly useful when documents with sensitive content are combined in a file cabinet.

Example:

The documents of the employees are stored in a personnel file cabinet. The employee name is available as an index entry. Human Resources employees have access to all documents, while individual employees only have access to documents that are stored with their names in the index data.

5.3 DocuWare as a High Security System

You can change a DocuWare System into a high security system. The organization administrator can then assign the high security property to certain users and file cabinets. Only a high security-user can access a high security file cabinet. There are some differences from a normal system:

- A user with the high security property, the password can no longer be reset by the organization administrator. Only the users themselves can change their password.
- A high security user cannot log on using a trusted login (see Chapter Login Methods), since with trusted login security is not ensured by DocuWare.
- If a file cabinet is set to "high security," it is no longer possible to assign file cabinet profiles to roles for these file cabinets, since file cabinet profiles must be assigned directly to users. These users must have the "high security" property. This prevents access to especially sensitive areas being granted by accident through uncontrolled groups and role assignments.

5.4 Encrypt Documents

To ensure that not even an administrator can read sensitive documents, DocuWare offers an encrypted storing of documents.

With this option you can also reliably prevent access to documents in the file system.

The key is 256 bits long by default. Key lengths of 192 or 128 bits are also available. The longer the key, the more secure the procedure, but the more time it takes for encryption and decryption and thus storage and search.

Note that encrypted file cabinets can only be accessed by authorized users. The document keys are decrypted using an asymmetric procedure with a key stored in the database. Since the documents cannot be decrypted without the key in the database, if you are using encrypted storage you should make sure that regular backups are made of the DocuWare system tables, so that the key tables in particular can be restored if the database is lost.

Additional information:

- Fulltext information is not encrypted by DocuWare. The index data in the database is also not encrypted. If the index data contains highly sensitive information, you should consult the options offered by the database provider - see also the following chapter.
- DWX files are not encrypted. In DWX files, metadata about the document can be saved in addition to being stored in the storage location of the file cabinet.

5.5 Protecting Sensitive Data Outside of DocuWare

Some of the data of DocuWare is unshielded and cannot be protected by specific DocuWare security mechanisms. This include the index data of the documents and the extracted full text, which are stored in their respective databases. Every system administrator with sufficient privileges to view the database can access these data. Fulltext is also stored in a separate index that is controlled by the fulltext server. The fulltext server is based on Apache SolR, a widely used fulltext engine.

If these data repositories contain sensitive data, then access to the databases, to the index location, and the access to the full text server URL - by default http://machinename:9012/solrt need to be restricted by the administrator using common methods such as access control lists for file directories or databases as well as a transparent Encrypted File System (EFS) for the fulltext user.

6 Integrity of Data and Documents

The integrity security objective states that data and documents must not be changed without authorization. All changes to a document must be traceable.

DocuWare guarantees the integrity of archived documents with the following measures:

- The rights system makes it possible to block documents for users generally or to make them accessible only to authorized users.
  You can also generally allow access to documents, but you can restrict it, for example by assigning users the right to read documents, but not the right to edit them.
  This has already been described in the chapter *Confidentiality* > *Rights* (on page 10).

- The *Automatic Version Management* file cabinet function allows you to check at any time whether a document has been changed.

- DocuWare can transparently log all user-related processes within a DocuWare system.

6.1 Document Version Management

If the *Automatically create new versions* function is enabled for a file cabinet, a changed document is saved as a new version in the same file cabinet. Every change of a document automatically leads to a new document version.

Both current and older versions are then located in the file cabinet. Older versions can be viewed in the version history which shows also the version numbers, the status, the storage date, any comments, and the user who saved the document.

The document being processed is checked out of DocuWare and locked. Other users can view the document, but cannot edit it until the document is checked in again as a new version. Only the current version can be edited.

It is also possible to set up version management so that individual documents are checked out manually and saved as new versions. Then, of course, the integrity of all documents in a file cabinet is not guaranteed.

More information about Version Management

6.2 Audit Reports

Audit reports give you full transparency of what is happening in your DocuWare system. With the appropriate permission, you can see, for example, who modified what configurations, or stored documents when.

All audit reports can be downloaded in universal CSV format and used for evaluations in many programs. Audit reports help you to evaluate activities in DocuWare and demonstrate compliance with compliance guidelines.

Examples of events logged at each level, including date, time, and user:

Document: Store, index change with old and new value, display, print, annotate, etc.

File cabinet: New index fields, changes to search and store dialogs as well as result lists, new file cabinet profiles etc. Also all document events within the file cabinet.

Organization: New configurations and changes to existing configurations, user login and logout (disabled by default)

System: Changes to server settings, changes to schedules for automatic processes such as transfer, deletion policies, synchronization

7 Availability of the DocuWare System

To ensure business continuity, a DocuWare system and its services should be fully operational. Users can access documents, data and applications at any time.

Since a document management system is usually embedded in a heterogeneous IT infrastructure, a failure can nevertheless occur for reasons that initially have nothing to do with the DMS - for example due to a hardware crash or an infection of client computers in the company with malware.

DocuWare however its protected by its special architecture:

- Scalability:
  Servers and other components can be installed multiple times so that redundant components can seamlessly take over functions that fail in the event of a hardware crash.

- DocuWare as a hybrid system:
  In addition to your on-premises system, DocuWare Cloud can serve as a redundant backup system and ensure business continuity in the event of a crash with virtually no downtime.
  To be able to switch seamlessly to the redundant system, the documents and index data must be regularly mirrored with the Synchronization module. All new and modified documents are transferred to the target, and documents deleted in the source can also be removed in the target. The mirroring process is via secure HTTPS (on page 8).
  The document versions, workflow history and log files are excluded from mirroring.

- Protection against malware:
  Cryptoviruses, for example, encrypt files in a file system so that they can no longer be used afterwards. When a user accesses synchronized cloud storage such as DropBox or Onedrive or a filesharing server with his infected computer, there is a risk that the virus will encrypt the entire contents of the cloud storage.
  This cannot happen with documents stored in DocuWare, as the files on the file storage are read and written exclusively by DocuWare server components. Only the account for DocuWare services requires write access. Since there is no bidirectional synchronization with the file system, a crypto virus on a client computer cannot cause any damage to the DocuWare system used.

8 Data Backup

Backup runs should be established for the data and documents in the DocuWare system so that the data can be restored immediately in the event of a hardware crash.

The backup of DocuWare databases and storage locations is the responsibility of the corporate IT department. There is no DocuWare mechanism that automatically backs up databases and storage locations.

8.1 Components That Have to be Backed Up Externally

The following DocuWare components must be backed up externally so that they are available again in the event of a hardware crash:

Databases

- DWSYSTEM: data relevant to the system and organization

- DWDATA: internal information for searching and finding documents

- DWNOTIFICATION: email notifications

Contents of the storage locations

A storage location is a file directory in the network or in a CAS system (Content Addressed Storage), in which documents and files from file cabinets and document trays, among others, are stored.

Fulltext text shots

The fulltext server stores the text shots in catalog files and uses them for the search queries. By default, they are stored on the computer on which the fulltext server is also installed. These catalog files can also be backed up as part of a backup and can be easily restored.

Further information on the structure and contents of the databases can be found in the White Paper System Architecture.

8.2 Backup of Document Metadata

All metadata of documents such as index data, annotations, stamps and signatures are automatically stored in the database and can be restored via an external database backup after hardware damage.

In addition, it is possible to save the metadata in the ZIP-based DWX format in the file cabinet's storage location. With the console application Restore Index Data, these redundantly stored metadata can be restored.

More information on document metadata in the White Paper System Architecture.