DocuWare

White Paper Document Security

September 2023

This document was created using AuthorIT™.

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.

Gender Neutral Communications

DocuWare communications are gender-neutral. All past and future communications issued by the company are inclusive of all genders, even if not explicitly stated in the wording.

DocuWare GmbH
Planegger Straße 1
82110 Germering
Germany
www.docuware.com

Contents

1 Objectives of this White Paper

Information security is increasingly becoming an important factor for the success of a company. However, while the protection of personal data is regulated in detail by law, companies and organizations can introduce different concepts to maintain information security.

The German Federal Office for Information Security (BSI) has published the IT-Grundschutz-Kompendium, a guide for companies and organizations on how to secure information and IT systems. Based on the requirements of ISO 27001 - the international standard for setting up an information security management system - this compendium lists three basic values, or protection goals, namely confidentiality, integrity and availability, which can be expanded depending on a company's risk assessment.

This white paper describes measures DocuWare as an Enterprise Management System offers for implementing these basic security objectives with regard to the documents archived in DocuWare:

- 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

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 document security of DocuWare on-premises system and in DocuWare Cloud. Where differences exist between the two systems, these will be referred to in detail.

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 on-premises
- 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 setting up a locally installed DocuWare system in the White Paper On-Premises

More information on setting up DocuWare Cloud in the White Paper DocuWare Cloud.

3.1 Login Methods

Using DocuWare always requires logging in to the DocuWare Identity Service first. As a central service, it is responsible for logging into DocuWare for all organizations within DocuWare. The user must identify himself as authorized via name and password.

The Identity Service enables authentication via single sign-on (SSO). The client logs on to the external provider, which in turn generates a token for the DocuWare Identity Service. This token is stored in the browser until it expires or the browser cache is cleared. When the token expires, the customer must log in again to obtain a new token.

Communication between the components is encrypted via HTTPS.

It is also possible to force single sign-on. This means that users no longer have the option of entering login data manually. By enforcing SSO within DocuWare, multi factor authentication (MFA) can also be indirectly enforced, provided MFA is set up at the identity provider.

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 the organization settings in DocuWare Configuration. 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.

It is recommended to set a minimum length of 14 characters for passwords as well as different character sets. It also increases security to use randomly generated passwords.

The administrator of the organisation can disable the password time limit again for specific users in the user administration area. 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 (page 10).

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).

In DocuWare Cloud, this is done automatically.

If you use a locally installed DocuWare system, you must carry out the following steps in IIS manager to configure the DocuWare Web components for HTTPS (SSL/TLS):

- 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.

DocuWare enables you to implement electronic signatures with different security levels. A DocuWare stamp with a signature on a document is an example of a simple signature. To provide the infrastructure for signing digital documents with the "advanced" and "qualified" higher security levels, DocuWare works with external signature service providers like Validated ID or DocuSign that offer multiple authentication options and numerous signature application functions, such as multi-signature or automatic reminder.

Read more about

- the technical background and how to configure signature workflows with Validated ID and DocuSign
- general information about security levels of signatures and how to use them

Workflows for electronic signatures with Validated ID and DocuSign can be implemented with both DocuWare Cloud and DocuWare on-premises.

5 Confidentiality: Document Access for Authorized Users Only

Employees often deal in a wide range of processes, even in small and medium-sized enterprises. In order to carry out their tasks, they need authorization to use a wide variety of resources, e.g., document and IT functions.

However, in order to achieve the security goal of "confidentiality", restrictions are also necessary. Certain restrictions make sure that only authorized personnel have the right to do certain things, and maintain transparency for everyone. Documents and data may only be viewed or modified by authorized users.

The following measures in DocuWare make it possible to implement such complex scenarios:

- Control document access via permissions (page 9).
- DocuWare as a high-security system (page 10) offers additional security through restrictions on the assignment of permissions. Only selected employees can access high security file cabinets. This prevents particularly sensitive areas in DocuWare from being accessed by mistake - for example, via incorrect groups and role assignments.
- Sensitive documents are protected from unauthorized access even at the administrator level thanks to standard 256-bit encryption (page 10).

Customers of locally installed DocuWare systems (on-premises) please note:

Certain data relevant to DocuWare cannot be protected with DocuWare permissions or other security measures. This includes the index data for the documents and the extracted full text that is stored in the respective databases.

To learn how to protect this information, please refer to the DocuWare On-Premises - System Architecture white paper in the Security and External Access chapter.

5.1 Permissions

The rights concept distinguishes between functional rights, file cabinet rights and object rights, which allow you to precisely control the scope of action of each user.

- Functional rights are permissions to certain program functionalities. This includes, for example, the right to create a stamp or a document tray. .
- 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.
- Object 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.

The various permissions are combined into profiles and assigned to individual or groups of employees.

Read more about how you can control the scope of action and document access with authorizations in the Basics article Permission concept.

5.2 DocuWare as a High Security System

To use DocuWare On-Premises as a high security system, the high security level must be activated once for the entire DocuWare system (*DocuWare Administration* > *System*). If you are using DocuWare Cloud, the high security level is enabled by default.

Both in DocuWare Cloud and in DocuWare On-Premises as a high security system an organization administrator can assign the high security property to certain users (*DocuWare Configuration* > *User Administration*) and file cabinets (*DocuWare Configuration* > *File Cabinets)*.

Only a high security-user can access a high security file cabinet.

There are some more differences from a system without a high-security level:

- 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.
- 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, since with trusted login security is not ensured by DocuWare.

5.3 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.

Please note specifically for DocuWare On-Premises:

- 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.
- 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.
- 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.

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 (valid for DocuWare Cloud and DocuWare as an on-premises system):

- 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. Read more in the article Permission concept of DocuWare.
- 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 (page 12) 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 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.

- For DocuWare Cloud, the backup and availability of data is ensured by DocuWare as the provider - find out more in the White Paper DocuWare Cloud.

Since a locally installed 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. 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. Find more information in chapter Availability and Data Protection in the White Paper DocuWare On-Premises.

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.

- For DocuWare Cloud, the backup and availability of data is ensured by DocuWare as the provider - find out more in the White Paper DocuWare Cloud.
- For locally installed DocuWare systems, 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. To find out which DocuWare components should be backed up externally in detail, please refer to the chapter Availability and Data Protection in the White Paper DocuWare on-premises.