OptimiDoc

OptimiDoc Cloud Security WhitePaper

version 23.05

OPTIMIDOC.COM

This document covers security and safety aspects concerning the usage of the OptimiDoc Cloud solution.

OptimiDoc develops the OptimiDoc Cloud to provide maximal safety and security of customer data and services provided. The best industry practices are utilised during the development, implementation and production stages of OptimiDoc Cloud.

Contents

1. OptimiDoc Cloud Security Quick Q&A

1.1. Data privacy

Can my reseller see any of my information?

Unless explicitly granted permission, resellers cannot access a customer's information. Some customers give their reseller support access as a managed service offering. Customers always have the control to revoke access for anyone at any time.

Can anyone see the content of my documents?

Nobody can see the content of your documents. We only keep the documents as long as needed. We delete it once we process the document and deliver it to the final destination.

Who owns my data?

You are the owner of the data. All data which comes from you to our system are yours.

Who can access my data?

You can decide who will see the information about your company. Admin rights can be assigned to specific users within your organisation. You can also provide admin rights to your service provider through the Support Partner option. Once you grant the Support partner rights to a company, they can manage your company. You have complete control to turn on or off the access.

OptimiDoc Cloud staff can access your company data in case of need:

- Legal Requirements
- Support requests
- System issues and bug resolution

If such access is needed, it's limited only to selected people and is prohibited except in the above circumstances.

Is my data encrypted?

All data transmitted between OptimiDoc Cloud components and customer infrastructure use TLS to encrypt all data in transit (TLS 1.2+ is used).

Microsoft Azure encrypts data stored in the OptimiDoc Cloud datacenter.

How is my data separated from other OptimiDoc Cloud customers' data?

Each company in OptimiDoc Cloud has a unique Identification Code assigned. All requests to OptimiDoc Cloud Datacentre must have a present ID next to other appliance info. Otherwise, the request is rejected. Additionally, all appliances need to be enabled by the administrator after the registration to OptimiDoc Cloud.

Next to the ID, every customer has also been assigned an encryption key to encrypt sensitive information, including stored documents or OAuth tokens, to access customers' cloud storage. Encryption keys are securely stored in key vault restricted access, except for the OptimiDoc Cloud application.

1.2. Architecture & Infrastructure

Where is OptimiDoc Cloud hosted?

OptimCapture Cloud Services are hosted in Microsoft Azure. Security is one of the critical factors for Microsoft, which was why we decided on it. For more information, check the Microsoft web: Azure Security | Microsoft Azure

Where is that data centre located?

We provide different data centres to fulfil the local legislation requirements. Currently, we have three basic ones, one in Europe, then in the US and Australia. Others can be added according to customer requirements.

Is infrastructure secured?

We are running complete infrastructure in the Microsoft Azure environment. Microsoft handles the physical security; the application-level security is actively monitored for security events by OptimiDoc using Microsoft Cloud Defender.

Who has access to data centres?

Only authorised OptimiDoc employees have access to the cloud infrastructure and the ability to deploy code changes. MFA (Multi-Factor Authentication) is a requirement for all OptimiDoc employees and is enforced on all cloud infrastructure access.

Is physical protection anticipated and designed with countermeasures applied?

OptimiDoc Cloud uses Microsoft Azure. Microsoft strategically selects datacenters locations to minimise the risks.

Does OptimiDoc Cloud have backups?

Yes, OptimiDoc performs daily backups.

What is the location of the data centre?

OptimiDoc Cloud has multiple data centres available for customers, which needs to fulfil the legal conditions.

Current locations are:

- European Union – Netherlands
- United States of America
- Australia

Where is the support and administration team located?

The support and Administration team of OptimiDoc Cloud is located in the Czech Republic. All documents and data are not transferred between the particular data centres or other locations.

1.3. Security

Are any penetration tests and code security done over the OptimiDoc Cloud?

Yes, we are performing automatic penetration tests over OptimiDoc Cloud. Code security/quality tools analyse every code change.

Do you have the ability to segment or encrypt customer data for specific customers logically?

All customer data are logically separated from other customers, and separate encryption keys encrypt sensitive data.

How is handled the access to my cloud storage?

OptimiDoc Cloud utilises the OAuth technology to authorise access to customers' cloud storage. Users' access and refresh tokens are kept in encrypted form inside the database. Users can easily revoke their access from the OptimiDoc Cloud Workplace web interface.

TLS encrypts complete communication between OptimiDoc Cloud and Cloud Storage.

Is OptimiDoc company certified by some security standard?

We are in the implementation phase of ISO 27001, and we expect to be finished in 2023.

How can I get more info?

Whenever you need more security information, please get in touch with our support at https://support.optimidoc.com.

2. Security responsibilities

OptimiDoc, partners and customers are together responsible for customer data security.

OptimiDoc is mainly responsible for the security of the following:

- Application development
- Physical protection
- Virtual infrastructure
- Data Security
- Backup and Log policy

Partners and customers are responsible for managing customers' accounts, users, rights and data governance. It requires strict compliance with all security and safety demands.

2.1. Application Development Security

OptimiDoc reviews strictly and validates the application source code to ensure the highest level of customer protection against any security incidents.

Source code analysis tools, also known as Static Application Security Testing (SAST) Tools, are used to analyse source code or compiled versions of code to help find security flaws.

Additionally, OptimiDoc performs penetration testing of OptimiDoc Cloud apps regularly.

Results of SATS and penetration tests are analysed, triaged, and prioritised. All necessary remediation steps are realised in a timely manner.

2.2. Physical protection

OptimiDoc outsources hosting its platform infrastructure to leading cloud infrastructure provider Microsoft and its Azure platform.

Microsoft Azure infrastructure meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. It also meets country or region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.

2.3. Virtual infrastructure

Virtual infrastructure security policy can be split into the following parts:

- **Network security**
  - Complete production infrastructure is isolated from non-production networks and other solutions provided by OptimiDoc. Direct access to virtual infrastructure is forbidden from non-production networks to servers and network devices in a production network.
  - Only temporary access from OptimiDoc offices is allowed to realise maintenance and upgrade operations.
- **Access policy**
  - OptimiDoc Cloud follows the principle of least privilege. Organisation responsibility is divided amongst organisations, and specific roles are assigned to manage those responsibilities.
  - MFA is required for all employees across the organisation.
- **Update and maintenance policy**
  - OptimiDoc periodically monitors and applies the latest application and operating security patches.
- **Intrusion protection**
  - Microsoft Azure Environment protects against network intrusion, data theft, and other threats like malware (even at the hardware level) and DoS attacks.

2.4. Data Security

Any access to customer data is strictly restricted except in reasonable cases. OptimiDoc Cloud staff can access your company data in case of need:

- Legal Requirements
- Support requests
- System issues and bug resolution

OptimiDoc Cloud uses Microsoft Azure Database. The database is accessible only from the OptimiDoc Cloud infrastructure (resource group). In the case of service tasks, access to a defined location is temporarily enabled. All accesses are audited in Audit logs and turned on by the Advanced Data Security service.

Data stored in OptimiDoc Cloud is encrypted and decrypted using a 256-bit AES encryption cypher - one of the strongest block cyphers available - and is FIPS 140-2 compliant. Print & Scan job data are stored temporarily only for the necessary time.

The complete OptimiDoc Cloud Azure infrastructure is separated into a defined resource group and continuously follows regulatory compliance standards.

OptimiDoc uses the industry standards TLS (1.2 and higher) protocols for data transfer to ensure data transmission security.

2.5. Backup and Log policy

Daily backups are performed over the OptimiDoc Cloud datacentres. Not all data is backed up; some data is transient and governed by strict lifecycle rules (i.e., print jobs stored in the Cloud Node or scan jobs waiting for delivery). As soon as the jobs are delivered, the data is permanently deleted. This minimises the period in which we retain potentially sensitive data.

Before any critical operations, such as OS/Application upgrading, architectural or security changes, necessary backup is taken.

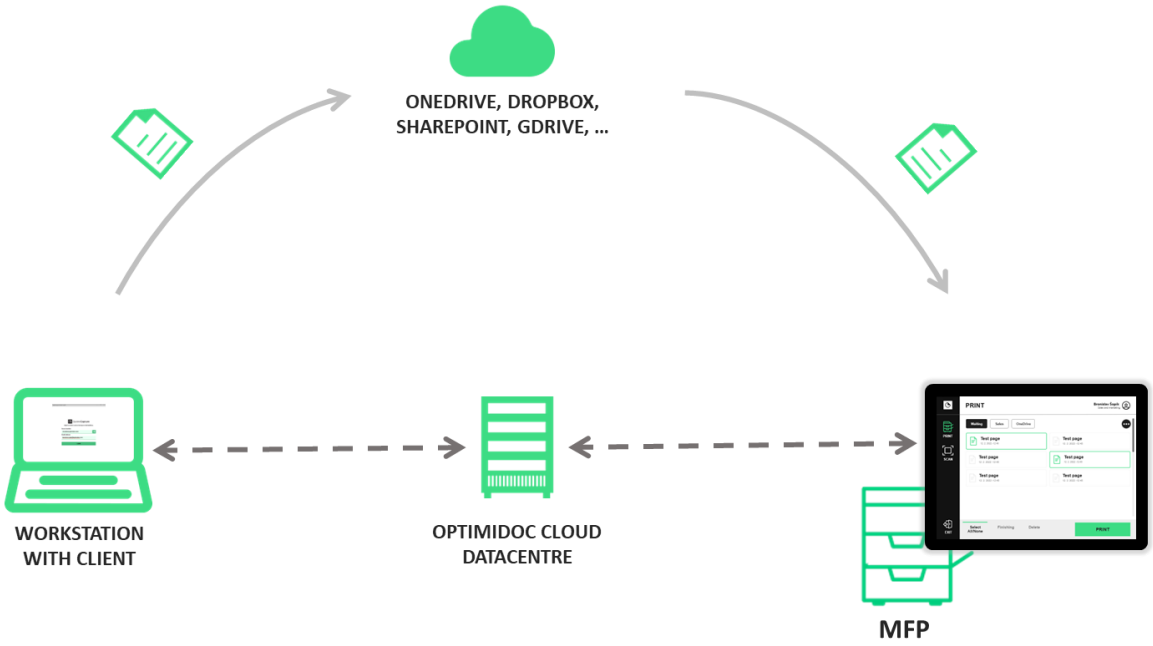
Necessary logs are maintained to track the user operations and instances' health checks.

2.6. OptimiDoc Cloud availability monitoring

OptimiDoc uses independent monitoring services to check the availability status of all services and datacentres. Monitoring services allow the registration of clients to obtain automatic email notifications in case of system failure.

The monitoring service also provides notifications of planned maintenance outages and incidents with resolution time.

3. Print process using customers' Cloud storage



Workstation with OptimiDoc Cloud Client (OCC)

- The user submits the document to print.
- OCC checks the document's final destination with the OptimiDoc Cloud datacentre and obtains a temporary Access token to the user's Cloud storage.
- OCC delivers the document to the user's cloud storage using the TLS protocol.
- After the document's successful delivery to cloud storage, OCC sends the metadata to the OptimiDoc Cloud datacentre.

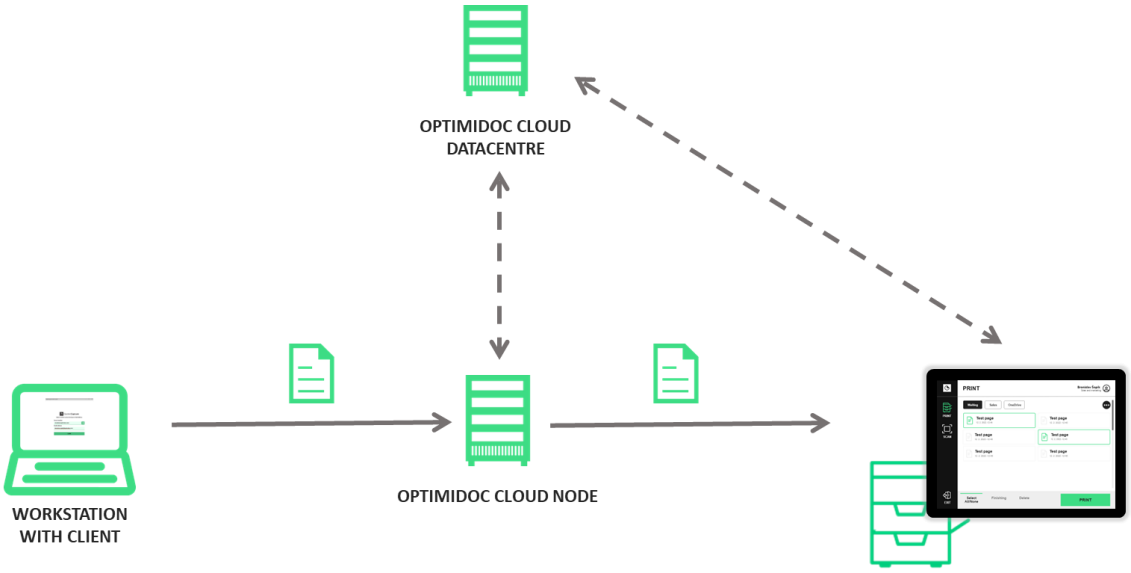
Multifunctional device with OptimiDoc Cloud Application

- User authenticates to OptimiDoc Cloud by one of the following methods:
  - Card
  - PIN
  - Account selection from a user list
  - Single Sign-On with 3rd party authentication application
    (Users can authenticate to OptimiDoc Cloud by using Single Sign-On if another 3rd party solution takes care of device authentication and provides the user information to the device.)
- The user releases the document using the OptimiDoc Cloud application
- OptimiDoc Cloud Application request the temporary URL address from the OptimiDoc Cloud datacentre.
- OptimiDoc Cloud Application downloads the document from the URL address using the TLS protocol and stores it locally.
- OptimiDoc Cloud Application releases the document on MFP,
- When the job is successfully released OptimiDoc Cloud Application notifies the OptimiDoc Cloud datacentre and sends accounting information using the TLS protocol. (accounting is not obligatory and may not be sent)

OptimiDoc Cloud Datacenter (OCD)

- OCD stores the accounting information
- OCD deletes the print document from cloud storage within the predefined period

4. Print process using OptimiDoc Cloud Node



Workstation with OptimiDoc Cloud Client (OCC)

- The user submits the document to print.
- The document is delivered to OptimiDoc Cloud Node through the LPR protocol.

OptimiDoc Cloud Node (OCN)

- OCN receives the document.
- Checks the user login with the user database in the OptimiDoc Cloud datacentre using TLS protocol.
- Stores the document in encrypted form.

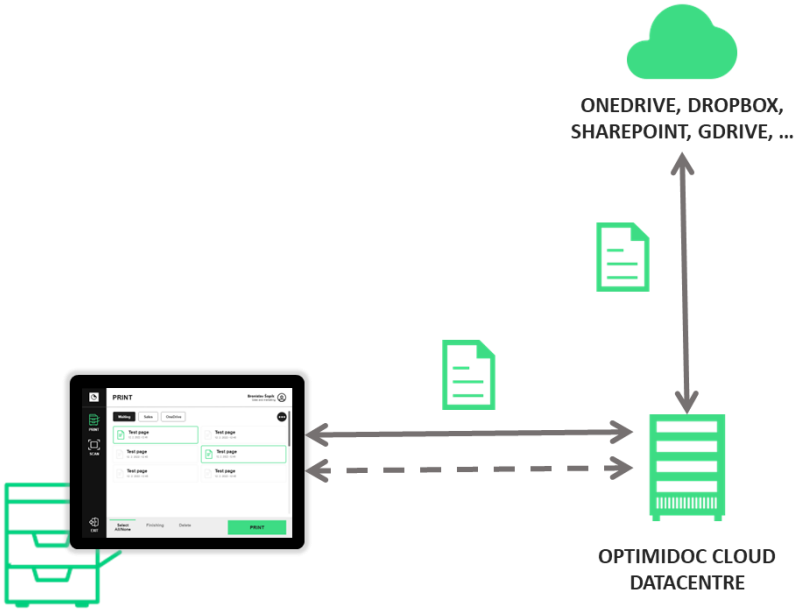
Multifunctional device with OptimiDoc Cloud Application

- User authenticates to OptimiDoc Cloud by one of the following methods:
  - Card
  - PIN
  - Account selection from a user list
  - Single Sign-On with 3rd party authentication application
    - (Users can authenticate to OptimiDoc Cloud by using Single Sign-On if another 3rd party solution takes care of device authentication and provides the user information to the device.)
- The user releases the document using the OptimiDoc Cloud application.
- When the job is successfully released OptimiDoc Cloud Application notifies the OptimiDoc Cloud datacentre and sends accounting information using the TLS protocol. (accounting is not obligatory and may not be sent)

OptimiDoc Cloud Node (OCN)

- OCN sends the document to the device through the LPR protocol.
- OCN deletes the document from storage.

5. Captured document processing to Cloud storage



MFP with OptimiDoc Cloud Integration

- User authenticates to OptimiDoc Cloud by one of the following methods:
  - Card
  - PIN
  - Account selection from a user list
  - Single Sign-On with 3rd party authentication application
    - (Users can authenticate to OptimiDoc Cloud by using Single Sign-On if another 3rd party solution is processing device authentication and providing the user information to the device.)
- The user selects a scan workflow.
- The user scans the document.
- The MFP creates the document image.
- The MFP sends document images and metadata to the OptimiDoc Cloud datacenter through TLS-encrypted HTTPS protocol.

OptimiDoc Cloud Datacenter

- Datacenter receives the document and stores it in encrypted storage.
- Based on processing settings, the document can be sent to the processing station for OCR, barcode recognition or advanced processing. Complete data transfer is done using TLS-encrypted HTTPS protocol.
- Datacenter starts the document delivery to the Cloud service
- OptimiDoc Cloud uses the OAuth for user authentication to particular Cloud storage.
- Before successfully delivering documents, users must authorise themselves with the selected Cloud storage.
  - User authorisation is done through the OptimiDoc Cloud user workplace web interface.
  - If the authorisation is successful, the cloud storage sends user-specific tokens to OptimiDoc Cloud.

    - OptimiDoc Cloud securely stores the user tokens in the database and uses them in the following automatic delivery of documents. User tokens are never provided to any 3rd party application or service.
    - Users can revoke the token anytime by visiting the Cloud storage site.

Cloud storage

- OptimiDoc Cloud stores the document once OAuth performs the user authorisation.

6. Communication paths & Encryption

The OptimiDoc Cloud provides and receives data from the following components:

- Workstation with OptimiDoc Cloud Client
- MFP device with OptimiDoc Cloud Application
- Network Printer
- OptimiDoc Cloud infrastructure
- Web browser
- OptimiDoc Cloud Client
- OptimiDoc Cloud Node
- Local Active Directory Sync tool

IMPORTANT
Components can be excluded in specific customer implementations.

Workstation with OptimiDoc Cloud Client > OptimiDoc Cloud

Purpose	Data	Protocol	Port	Encryption
Delivery of print job to the virtual spooler. OptimiDoc datacentre used storage.	- Print data (PCL/PS/XPS/PDF) - Login&Password	IPPS	443	TLS
OptimiDoc Cloud Client communication	- Printer list - Temporary access tokens to Cloud storage - Authentication process	HTTPS	443	TLS

Workstation with OptimiDoc Cloud Client > Printer

Purpose	Data	Protocol	Port	Encryption
Delivery of print job	- Print data (PCL/PS/XPS/PDF) - Login&Password	LPR	515	NO

Workstation with OptimiDoc Cloud Client > Cloud storage

Purpose	Data	Protocol	Port	Encryption
Delivery of print job	- Print data (PCL/PS/XPS/PDF) - Login&Password - OAuth token	HTTPS	443	TLS

Workstation > OptimiDoc Cloud Node

Purpose	Data	Protocol	Port	Encryption
Delivery of print job	- Print data (PCL/PS/XPS/PDF) - Login&Password	LPR	515	NO

MFP device > OptimiDoc Cloud

Purpose	Data	Protocol	Port	Encryption
Authentication & authorisation of the user	- Login and password or PIN or Card - Email - Full name - Access rights	HTTPS	443	TLS
Embedded application communication	- Specific data requests in scan and print application	HTTPS	443	TLS
Delivery of scanned document	- Scan document data - Scan document description file with user login and metadata	HTTPS	443	TLS
Print documents download	- Print data (PCL/PS/XPS/PDF)	HTTPS	443	TLS
Accounting data	- Login - Document name - Accounting information	HTTPS	443	TLS
MFP authentication	- Company Identification Code - Access token - Serial number	HTTPS	443	TLS

MFP device > OptimiDoc Cloud Node

Purpose	Data	Protocol	Port	Encryption
Authentication & authorisation of the user	- Login and password or PIN or Card - Email - Full name - Access rights	HTTPS	443	TLS*
Print job request	- Login	HTTPS	443	TLS*

IMPORTANT*
OptimiDoc Cloud Node default algorithm used for Encryption is SHA1 with the self-signed certificate.

MFP device > Cloud storage

Purpose	Data	Protocol	Port	Encryption
Print documents download	- Print data (PCL/PS/XPS/PDF)	HTTPS	443	TLS

OptimiDoc Cloud > Other services

Purpose	Data	Protocol	Port	Encryption
Delivery and download from Cloud storage	- Scan document - Access/Refresh token - Metadata - Email	HTTPS	443	Cloud storages defined
Azure AD sync	- Login - Email - Full name - Department - Card - PIN	HTTPS	443	Microsoft AzureAD defined
Cloud storages authentication through oAuth2.0	- Access token - Refresh token	HTTPS	443	Cloud storages defined

OptimiDoc Cloud Node <> OptimiDoc Cloud

Purpose	Data	Protocol	Port	Encryption
User authentication data	- Login - Pin - Card - Access rights	HTTPS	443	TLS
Print data	- Print data (PCL/PS/XPS/PDF)	HTTPS	443	TLS
Remote authentication	- User login - Email - Full name - Access rights	HTTPS	443	TLS
Accounting data (only Xerox)	- JBA log	HTTPS	443	TLS
OptimiDoc Cloud Node authentication and configuration	- Company Identification Code - Access token - Serial number - Service-specific information	HTTPS	443	TLS

OptimiDoc Cloud Node > MFP

Purpose	Data	Protocol	Port	Encryption
Accounting data (only Xerox)	- JBA log	HTTPS	443	Device defined
Print documents delivery	- Print data (PCL/PS/XPS/PDF) - User login	LPR	515	No
Remote authentication	- User login - Email - Full name - Access rights	HTTPS	443	TLS

OptimiDoc Cloud Node > Cloud storage

Purpose	Data	Protocol	Port	Encryption
Print documents download	- Print data (PCL/PS/XPS/PDF)	HTTPS	443	TLS

Local Active Directory Sync tool > Local Domain Server

Purpose	Data	Protocol	Port	Encryption
Lightweight Directory Access Protocol synchronisation	- Login - Email - Full name - Department - Card - Pin	LDAP	389,3268	No
		LDAPS	636, 3269	LDAP defined

Complete communication between the OptimiDoc Cloud internal components is secured through TLS. The default algorithm used for Encryption is SHA256, with a signed certificate from Sectigo RSA Domain Validation Secure Server CA. The minimal TLS version is 1.2.