fenestrae®

Udocx Security Factsheet

Contents

Introduction

Udocx (www.udocx.com) is a cloud-based document capture and processing solution. With Udocx, you can easily digitize paper documents, send them via Office 365 email, or store them in Microsoft OneDrive or SharePoint. Udocx is a solution from Fenestrae, a Microsoft Independent Software Vendor (ISV) and Gold Certified Partner with headquarters in The Hague, The Netherlands.

Core Design

The core design of Udocx maximizes both data security and service availability. As a true cloud-based solution, Udocx features virtually unlimited service bandwidth, geographically redundant datacenters, and the latest technologies to block DDoS and other common cyber-attacks. Only secure and encrypted (SSL/TLS) connections are allowed, and all unencrypted connection attempts are ignored.

It's important to understand, from a security perspective, that Udocx does not store client documents. It's best to think of Udocx as an intelligent document acquisition and routing engine – the interface between your multi-functional peripheral (MFP) devices and your data storage infrastructure. Digitized documents are not retained by Udocx once they have been successfully delivered to their Email/OneDrive/SharePoint destination.

Document Storage

Udocx is an intelligent document acquisition and routing engine. It is NOT a document storage service.

Udocx processes scanned documents and delivers them, securely and automatically, to destinations defined by the customer. A destination can be one or more email recipients, or the current user's email drafts folder, a OneDrive folder, or a SharePoint document library.

Scanned documents are processed in the Udocx data center. The document processing steps are:

- Normalize the scanned image(s)
- Convert the scanned image(s) into an industry-standard PDF/A (when not already PDF/A)
- Deliver the resulting document to the chosen destination

After processing, the document is delivered to the destination via HTTP/s. When the destination supports metadata, such as a SharePoint document library, this data can be hardcoded into the Udocx app or provided by the customer at scan time. The metadata fields are populated when the document is delivered.

When the destination application confirms that the document has been successfully delivered, the document is completely removed from Udocx. If a scanned document cannot be delivered to the specified destination, after several retries (based on the nature of the failure), the resulting PDF/A is sent as an email attachment to the originating user as part of a failure notification. Again, the document is completely removed from Udocx.

Document Format

When a document is scanned on the MFP, the Udocx service receives one or more images which represent each page of a given document. These images are verified, normalized, and assembled by Udocx into a PDF/A file. If the scanned document is delivered to Udocx already in PDF/A format, the original document is used. In either event, each scan operation results in a single PDF/A file.

The PDF (portable document format) standard was originally published in 1993 as a method of describing documents that was both application and hardware independent. In 2005, the International Organization for Standardization (ISO) defined PDF/A specifically for archival use. PDF/A does not allow audio/video content, JavaScript or any type of code execution, external content references, or document-level encryption. All fonts must be embedded, images must use specific compression formats, and any included metadata must conform to the XMP (eXtensible Metadata Platform) ISO standard.

PDF/A eliminates the potential for malicious code execution, controls file sizes by forbidding “bloat” features such as audio/video, and ensures that your documents are “futureproof” and accessible for decades to come.

Transaction Logs

While Udocx does not retain processed documents, it does keep a transaction log of each operation for troubleshooting and accountability purposes.

No information regarding the content of the scanned documents is retained in the transaction log.

User Access

In addition to the Udocx interface on the MFP, users also have access to the Udocx User Portal through any standards-compliant Internet browser. The portal allows the users to customized their own Udocx applications and scan destinations without the need for an administrator.

Application Access

Udocx integration with Office 365 (Email/OneDrive/SharePoint) is based on standard APIs published by Microsoft. All communications are encrypted using HTTP/s with TLS version 1.2.

User access to Office 365 is based on OAuth (Open Standard for Authorization). When a user creates an application through the Udocx User Portal, they grant permission for the Udocx service to interface with Office 365 on their behalf. This type of pass-through authentication means that Udocx has the same Office 365 access that the current user has – no more and no less. There are no "super user" accounts in Udocx.

Infrastructure Protection

Udocx is a true cloud-based application running within the Microsoft Azure infrastructure. Azure's infrastructure security includes hardware, software, networks, administrative and operations staff, and the physical datacenters that house it all.

Azure runs in geographically distributed Microsoft facilities. Each facility is designed to run 24/7, 365 days a year, and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.

- **Update management.** Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for all Microsoft software.
- **Anti-virus and anti-malware.** All Udocx servers run anti-malware solutions provided by Microsoft.
- **Penetration testing.** Datacenter personnel conduct regular penetration testing to improve security controls and response processes.
- **DDoS Protection.** Udocx has a built-in defense system against Distributed Denial-of-Service (DDoS) attacks on the platform and uses standard detection and mitigation techniques. Additionally, Azure's own DDoS defense system guards against attacks from both inside and outside the platform.

Data Protection

Udocx is a multi-tenant service, meaning that multiple customer deployments and virtual machines are stored on the same physical hardware. Data protection includes:

- **Data separation.** Each customer can only be access their own data.

- **Encryption.** Data in storage is encrypted to align with business practices for protecting confidentiality and data integrity. For data in transit, Udocx uses secure, industry-standard transport protocols between devices and within datacenters themselves.

- **Data destruction.** When customers delete data or leave Udocx, Fenestrae follows strict standards for overwriting storage resources before reuse.

Certifications and attestations

Udocx uses the Microsoft Azure platform which includes contractual privacy commitments that help assure client privacy. The Microsoft Azure infrastructure runs in an ISO 27001 certified datacenter. Datacenters with this certification are designed for business productivity public cloud service and have implemented a rigorous set of global standards covering physical, logical, process, and management controls. In addition to ISO 27001, Udocx on the Microsoft Azure platform also adheres to the following global standards:

- **ISO/IEC 27018. ISO/IEC 27018** code of practice. Covering the processing of personal information by cloud service providers.

- **ISO/IEC 27001/27002:2013.** The standard that defines the security controls required of an information security management system.

- **EU Model Clauses.** The EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU. The EU's Article 29 Working Party ensures this. In accordance to this article the contractual privacy protections Fenestrae delivers to its customers meet current EU standards for international transfers of data.

- **US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Program.** Frameworks set forth by the US Department of Commerce regarding the collection, use, and retention of data from the EEA and Switzerland.

- **PCI DSS.** Udocx can be configured to support Level 1 compliancy with Payment Card Industry (PCI) Data Security Standards (DSS) version 3.0, the global certification standard for organizations that accept most payments cards, as well store, process, or transmit cardholder data.

- **SOC 1 and SOC 2.** The Service Organization Control (SOC) reporting framework for both SOC 1 Type 2 and SOC 2 Type 2.

- **UK G-Cloud.** The UK Government G-Cloud is a cloud computing certification for services used by government entities in the United Kingdom.

- **CDSA.** The Content Delivery and Security Association (CDSA) provides a Content Protection and Security (CPS) standard for compliance with anti-piracy procedures governing digital media.

- **CSA CCM.** The Cloud Security Alliance (CSA) is a non-profit, member-driven organization with a mission to promote the use of best practices for providing security assurance within the cloud. The CSA Cloud Controls Matrix (CCM) provides detailed information about how Azure fulfils the security, privacy, compliance, and risk management requirements defined in the CCM version 1.2, and is published in the CSA's Security Trust and Assurance Registry (STAR).

For a complete overview of the certifications and attestations, see:

https://www.microsoft.com/en-us/trustcenter.

Need more information?

Phone: +31 70 3015 100

Email: info@udocx.com

Web: www.udocx.com.