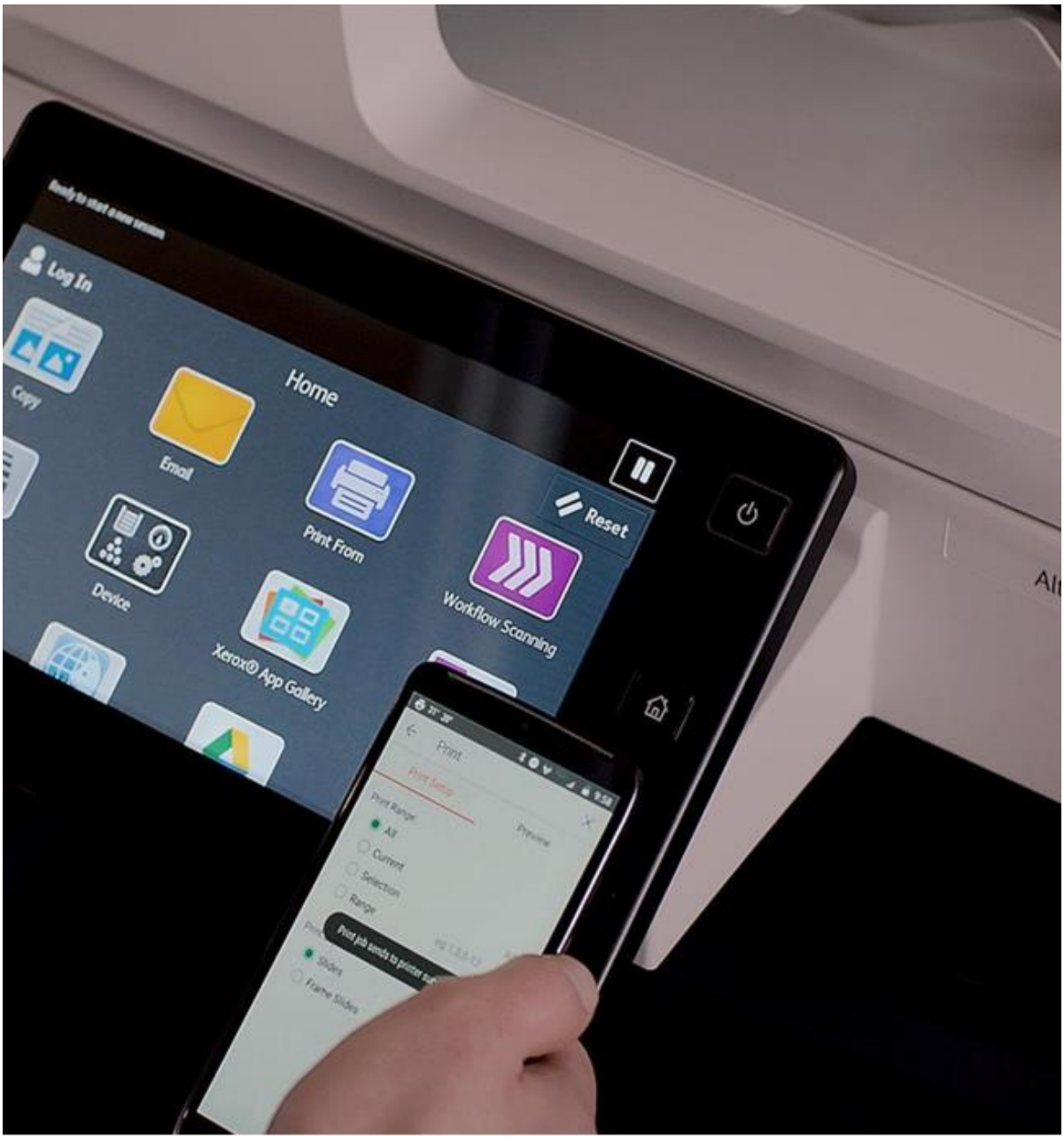
Security Guide

Xerox® Intelligent Filer App



xerox™

Document Version: 20230801

Contents

1. Introduction

Purpose

Xerox® Intelligent Filer is a Xerox Gallery App that lets users extract data and classify documents with ease. Using a variety of classifiers and extractors that have been custom trained for document types like Invoices, Bills, and Bank Statements, Intelligent Filer processes your scanned documents and suggests a document type based on the content. Then, by using pre-defined or custom templates, Intelligent Filer suggests a document name and folder location based on the data that has been extracted from the document and then uploads it to the Cloud repository of your choice – OneDrive, MS365/SharePoint, Google Drive, DocuShare Go US, or DocuShare Go EU.

Intelligent Filer also supports Xerox SSO for a quick and efficient sign-in process.

The purpose of the Security Guide is to disclose information for Xerox® Intelligent Filer with respect to device security. Device security, in this context, is defined as how data is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. This document describes the design, functions, and features of Xerox® Intelligent Filer relative to Information Assurance (IA) and the protection of customer-sensitive information. Please note that the customer is responsible for the security of their network and Xerox® Intelligent Filer does not establish security for any network environment.

This document does not provide tutorial-level information about security, connectivity, or Xerox® Intelligent Filer features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security. It is assumed that the reader is familiar with the apps; as such, some user actions are not described in detail.

Disclaimer

The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

2. Product Description

Overview

Xerox® Intelligent Filer consists of one primary workflow:

- Scan and file a document

The app and workflow facilitate a combination of the following steps:

- App Components
- App Gallery Configuration
- Sign-In
- Xerox Single Sign On (SSO)
- Document Type Configuration
- Browse
- Scan, Process, and Persist
- Logging
- SNMP & Device Webservice Calls

App Components

Xerox® Intelligent Filer consists of five key components: the EIP web app, the EIP weblet, the REST API, the database, and blob storage.

The user installs the EIP weblet from the App Gallery onto a Xerox device. When a user runs the weblet, the EIP web app launches.

The REST API interacts with the Xerox Cloud Repository Middleware. The Cloud Repository Middleware component is a service hosted on the Microsoft Azure Cloud System. The Cloud Repository Middleware interfaces with the following commercial cloud repository providers: Xerox® DocuShare® Go Content Management Platform, Microsoft (OneDrive and MS365/SharePoint), and Google Drive.

The REST API also interacts directly with Aluma.io's platform for document processing.

See **User Data Protection within the Product** on page 7 for details on hosting.

App Gallery Configuration

Before you can run Intelligent Filer on your Xerox® device(s), you must configure the app using App Gallery configuration. When you install the app for the first time, you will be prompted to specify:

- SNMP community name
- The Cloud repository you would like to connect the app to – OneDrive, MS365/SharePoint, Google Drive, DocuShare Go US, or DocuShare Go EU.
- If you choose MS365/SharePoint as the Cloud repository, you will need to provide the site name.

These values are passed by the EIP weblet to the EIP web app on app startup and are stored in local storage on the Xerox device.

Sign-In

When Intelligent Filer is opened on the Xerox® device, the EIP web app sends the REST API details of the user's configuration, including the Cloud repository specified in App Gallery, which determines which OAuth sign-in screen the user is presented with – Microsoft, Google, DocuShare Go US, or DocuShare Go EU. This call with the configuration details inititates a token exchange and redirect process with the 3rd party via the Xerox Cloud Repository Middleware to complete sign-in.

Xerox Single Sign On (SSO)

If a user is leveraging Xerox Workplace Suite (XWS) or Xerox Workplace Cloud (XWC), they can use Xerox SSO to sign into the app. This works by storing the user's auth token within Xerox Workplace Suite or Xerox Workplace Cloud.

Document Type Configuration

Intelligent Filer currently supports the following document types – Invoices, Bills, Delivery Notes, Agreements, Bank Statements, Correspondence, and Miscellaneous. Each document type comes with a default, pre-configured template for automatic document naming and folder specification.

The default document template defines the structure of the document name, which can include static words or characters, as well as variables that will automatically populate with values that are extracted from the scanned documents.

The default folder defines where in the Cloud repository the document should be filed to.

Both the default document name and default folder are unique to each document type and can be modified by the user on the device.

The default document name and default folder are stored in local storage on the Xerox device.

Browse

During the workflow, users have the opportunity to browse and search the folders and files associated with their Cloud repository account. The REST API fetches this information from the Xerox Cloud Repository Middleware. Users can also create new folders.

Scan, Process, and Persist

When a user scans a document, it is temporarily stored in Azure blob storage and sent to Aluma.io for processing. Processing includes OCR (Optical Character Recognition), document classification, and data extraction.

OCR is used to make the output PDF searchable.

Document classification suggests the document type.

Data extraction pulls key values from the document to be used as variables in the document name.

Once processing is finished and the user has completed the app's workflow, the searchable PDF is uploaded to the user's Cloud repository via the Xerox Cloud Repository Middleware.

Logging

Logging is persisted on the server to aid with support and application scaling. Logging is transmitted over TLS.

SNMP & Device Webservice Calls

During standard usage of Intelligent Filer, local calls to SNMP are initiated to pull relevant details such as device language. The initiation of scan and the usage of internal graphical components are also handled through these device-level web service calls.

3. User Data Protection

User Data Protection within the Product

The Xerox® Intelligent Filer EIP web app, REST API, database, and blob storage are hosted on the Microsoft Azure Network in both the US and Europe.

The EIP weblet is hosted in the Xerox App Gallery.

The Xerox Cloud Repository Middleware, which Intelligent Filer uses for all calls to OneDrive, MS365/SharePoint, Google Drive, DocuShare Go US, and DocuShare Go EU, is also hosted on the Microsoft Azure Network in both the US and Europe.

Aluma.io's platform is hosted on the Google Cloud Platform in Europe.

Microsoft's Azure and Google's data center operations feature comprehensive information security policies and processes using standardized industry control frameworks, including ISO 27001, SOC 1, and SOC 2.

For a full description of Azure's security, please follow the link: https://docs.microsoft.com/en-us/azure/security/azure-network-security.

For a full description of Google's security, please follow the link: https://cloud.google.com/security.

For more information regarding user data protection provided by the Xerox® Multifunction Device, please reference your specific model's Security Guide.

User Data at Rest

Data Persistence

Scanned documents are temporarily stored in Azure Blob storage for 15 minutes.

When a document is passed to Aluma.io for processing, it is stored by Aluma in dynamic memory (in a memory-only Redis cache) and is never saved to disk. It remains in dynamic memory only for a few seconds, until processing is complete, and is then immediately deleted.

Data that is extracted from a scanned document is stored temporarily in Intelligent Filer's database. This data is encrypted using AES-256.

Local storage on the Xerox device is used to persist the user's most recent scan settings, Document Type configuration values, as well as values from App Gallery and App Gallery Configuration, such as app ID, device serial number, SNMP community name, Cloud repository, and MS365/SharePoint site name. Local storage on the Xerox device is not accessible by the user.

Logging is persisted on the server to aid with support and application scaling.

User Data in Transit

Secure Network Communications

The Xerox® Intelligent Filer EIP web app and REST API require that the device can communicate over port 443 outside the client's network. All communication between the application and outside services is over HTTP Secure (TLS).

The scanned document and extracted information is sent securely to/from the REST API, database, Azure Blob storage, Aluma.io's platform, and the Xerox Cloud Repository Middleware, which interacts with OneDrive, MS365/SharePoint, Google Drive, DocuShare Go US, or DocuShare Go EU, depending on the configuration. The document being transmitted could contain PII.

If the user is leveraging Xerox SSO, the device session username is retrieved from the device and sent to Xerox Workplace Suite/Cloud.

4. Additional Information and Resources

Security Xerox

We maintain an evergreen public web page that contains the latest security information pertaining to its products. Please see https://www.xerox.com/security.

We have created a document that details the Xerox Vulnerability Management and Disclosure Policy used in the discovery and remediation of vulnerabilities in Xerox® Software and Hardware. It can be downloaded from this page: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html.

Additional Resources

Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/

Table 1 Security Resources