Xerox®
Security Guide
for Auto-Redaction App

Document Version: 2.0 (April 2019).

Table of Contents

1 Introduction

Purpose

Xerox® Auto-Redaction App is a solution that allows users to redact certain information from their scanned document, straight from a Xerox® Multifunction Printer (MFP). Phone numbers, Social Security Numbers, emails, names, and more can all be redacted with the touch of a few buttons.

The purpose of the Security Guide is to disclose information for Xerox® Auto-Redaction App 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 design, functions, and features of Xerox® Auto-Redaction App 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® Auto-Redaction App does not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity or Xerox® Auto-Redaction App 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 Xerox® Auto-Redaction App; 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® Auto-Redaction App consists of two primary workflows. The two workflows being:

- Redact a document
- Redact a document using a preset

The two workflows facilitate a combination of the following steps:

- App Hosting
- Selection
- Scanning
- Printing
- Emailing
- SNMP & Device Webservice Calls
- OCR, Data Redaction, and Document Conversion

App Hosting

Xerox® Auto-Redaction App consists of three key components; the device app, the API, and the associated database. The device app is a ConnectKey® / EIP webapp and the API is a REST API.

Selection
At various steps in the application the user may be prompted to make selections. These selections include standard and custom info types as well as scan settings. They are dynamic and are driven by API calls.

Scanning
When scanning, documents are scanned and submitted to the API. Due to the nature of the Xerox® EIP scanning workflow design, the user's scan is temporarily persisted while OCR and redaction is completed by the API. The resulting redacted document is also temporarily persisted for use with email and print.

Printing
When printing, the temporarily persisted redacted document is pulled from the API.

Emailing
Once the redaction is complete, the user can send the resulting document to an email address they specify.

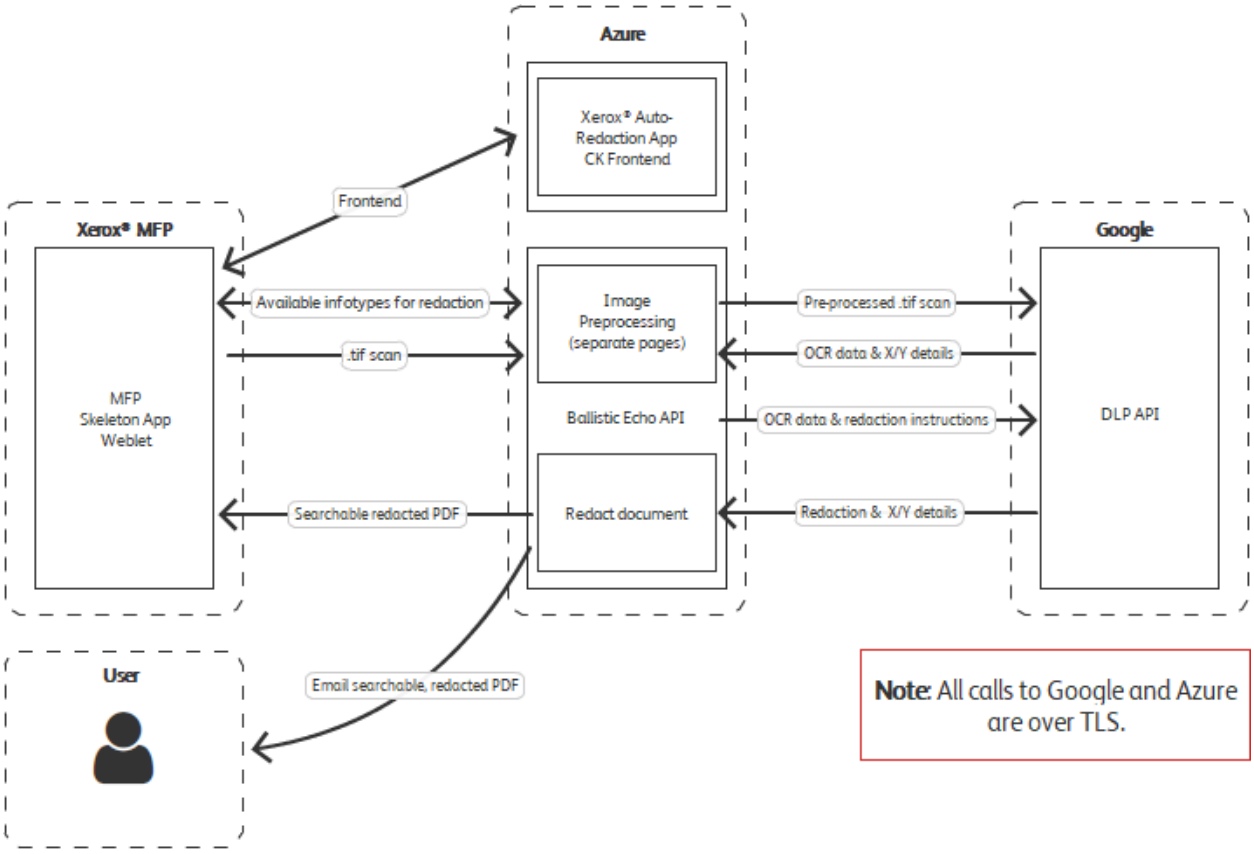
SNMP & Device Webservice Calls
During standard usage of Xerox® Auto-Redaction App, local calls to SNMP are initiated to pull relevant details such as device language. The initiation of scan, print, and the usage of internal graphical components are also handled through these local web service calls.

OCR, Data Redaction, and Document Conversion
During the OCR and data redaction stage, the API leverages Google's Cloud Vision and DLP (data loss prevention) services.

Architecture and Workflows

Architecture Diagram

Below is a diagram that outlines what data is being processed and transmitted between each service.



3 User Data Protection

User Data Protection within the product

Xerox® Auto-Redaction App API and EIP app are hosted on the Microsoft Azure Network. Microsoft's Azure 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, please follow the link: https://docs.microsoft.com/en-us/azure/security/azure-network-security

User Data in transit

Secure Network Communications

Xerox® Auto-Redaction App and API require that the device can communicate over port 443 outside the client's network. All web communications between the API, Google services, and Xerox® devices are encrypted using HTTP Secure (HTTPS).

Documents that are scanned are temporarily stored as Azure blobs (raw image, thumbnails, etc.). The raw image is not accessible from anything other than the server-side code.

The thumbnails are stored using short live Secure Access Signature URLs but are not encrypted for convenience and performance. Once the user is finished processing, they are removed.

During the processing of a document, a document bundle is stored. All detail about the document, such as data from OCR, and images are temporarily persisted. Once the user has finished, all document details are deleted.

4 Additional Information & Resources

Security @ Xerox®

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

Responses to Known Vulnerabilities

Xerox® has created a document which details the Xerox® Vulnerability Management and Disclosure Policy used in 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

Below are 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/