Security Guide

Xerox® Summarizer App

Contents

1. Introduction

Purpose

Xerox® Summarizer App creates a summary of documents for viewing, printing, and emailing, right on a Xerox® Connect Key® enabled device. With the help of artificial intelligence (AI), Xerox Summarizer reduces dozens or even hundreds of pages by a percentage of the original text (extractive) or a short and concise interpretation of the source text (abstractive). You can easily preview your summary on the fly, adjust the summary length, and email the result in PDF or Microsoft Word format.

The purpose of the Security Guide is to disclose information for Xerox® Summarizer 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® Summarizer 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® Summarizer App does not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity, or Xerox® Summarizer 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 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® Summarizer App consists of two primary workflows:

- Create an extractive summary
- Create an abstractive summary

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

- App components and hosting
- Scan
- Preview
- Print
- Email
- Logging
- SNMP & Device Webservice Calls

App components and hosting

Xerox® Summarizer App consists of five key components: the Xerox Extensible Interface Platform® (EIP) web app, the EIP weblet, the REST API, the database, and blob storage.

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

Scan

When a user scans a document, the scan images are submitted to Google's Cloud Vision API for OCR. The scan images are stored in Google Cloud Storage for a maximum of 15 minutes. Once OCR is complete, the data is sent to SummarizeBot for processing and summarization.

Preview

Users have the option to view a preview of their summary before emailing or printing the result. Previews are generated using the data from SummarizeBot's API.

Print

Users have the option to print their summary. Print jobs are retrieved via the REST API using a unique, time sensitive, complex identifier, and could contain sensitive information.

Email

Users can choose to email their summary and original document as a PDF or DOCX file. If enabled, an email will be sent to the specified email address(es) with a link to download the summary. Summary output (which may include the original document) is stored in Azure blob storage for 7 days to maintain email link integrity.

No email configuration is required. The email will be sent from a noreply Xerox email address.

Logging

Logging is persisted on the server to aid with support and application scaling. Logging is transmitted over TLS and no personally identifiable information is stored.

SNMP & Device Webservice Calls

During standard usage of Summarizer, 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® Summarizer EIP web app, REST API, database, and blob storage are hosted on the Microsoft Azure Network. The EIP weblet is hosted in the Xerox App Gallery.

Google's Cloud Storage and Vision API are hosted with Google.

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 on Azure's security, please follow the link: https://docs.microsoft.com/en-us/azure/security/azure-network-security.

For a full description on 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

Scan images are stored in Google Cloud Storage for a maximum of 15 minutes. Summary output (which may include the original document) is stored in Azure blob storage for 7 days to maintain email link integrity.

Local storage on the Xerox® Device is used to persist email addresses and the previously selected domain for convenience.

Usage statistics are stored in the database. Statistics include number of jobs, number of pages per job, and whether the job was an extractive or abstractive summary. These statistics do not contain PII.

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

User Data in Transit

Secure Network Communications

The Xerox® Summarizer web app and REST API require that the device can communicate over port 443 outside the client's network. All communication between all aspects of the application are encrypted using HTTPS Secure (TLS version 1.1 and 1.2).

The document to be summarized is sent to/from the REST API, Google's Cloud Vision API, Google Cloud Storage, and SummarizeBot's API. The document could contain PII.

4.   Additional Information and 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 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