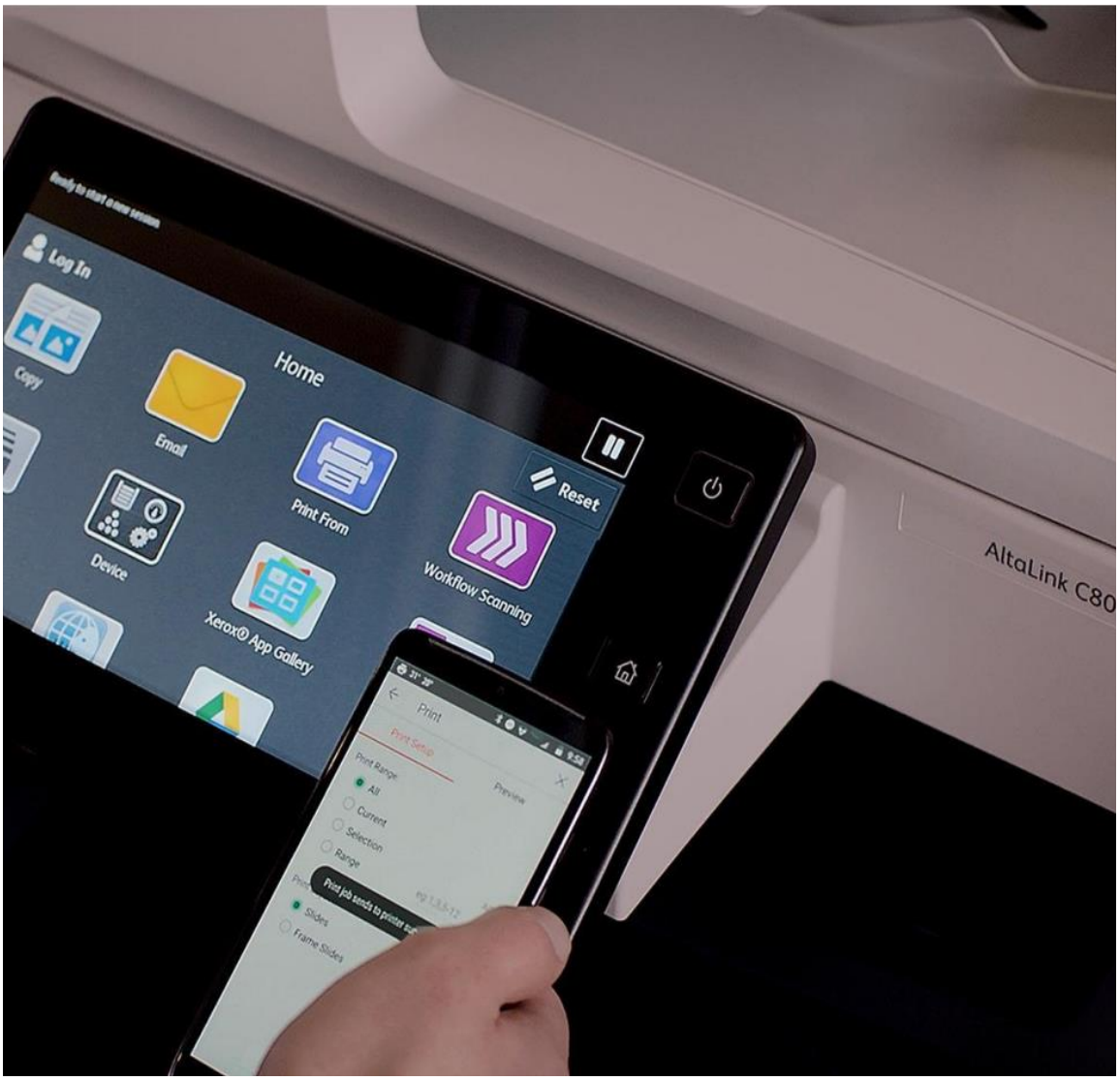
Xerox® Security Guide

Connect App for Sage Accounting



xerox™

Document Version: 1.0 (September 2019).

Table of Contents

1. Introduction

Purpose

Xerox® Connect App for Sage Accounting (Connect for Sage Accounting) is a Xerox® Gallery App that allows users to connect to their Sage Business Cloud Accounting account, right on the device. Xerox® Workplace Solutions (Xerox® Workplace Suite and Xerox® Workplace Cloud) works as the Single Sign-On mechanism, making sign-in fast and easy. Using Google's Invoice Capture technology, the app will automatically pull details off a user's vendor invoice, and then use those details as data to create the invoice within Sage. Alternatively, the user can scan and attach a payment, such as a check or check stub, to an existing, outstanding invoice.

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

This document does not provide tutorial level information about security, connectivity or Xerox Connect App for Sage Accounting 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 Connect App for Sage Accounting consists of two primary workflows. The two workflows are:

- Scan a Vendor Invoice
- Scan a Payment

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

- Single Sign-On
- App Hosting
- Selection
- Scanning
- Intelligence
- SNMP & Device Webservice Calls

Single Sign-on

If a user is leveraging Xerox Workplace Suite or Cloud, the user can use Single Sign-On to sign into the app. This works by storing the user's Sage sign-in token within Workplace Suite/Cloud.

App Hosting

Xerox Connect App for Sage Accounting consists of three key components: the device app, the API, and the associated database. The device app is a ConnectKey®/EIP web app 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 Sage invoice fields, such as vendor/contact, due date, ledger account, description, and tax rate. They are all dynamic and are driven by API calls. The user will select various scan settings before scanning their document, too.

Scanning

With the vendor invoice workflow, invoices are scanned and submitted to Google's Invoice Capture API for processing. Data is sent back from Google, which is used to help fill vendor invoice fields, like contact and subtotal. The scanned image in both workflows is sent to Sage's API for upload and attachment. We will temporarily persist the scanned image while in transit to/from Sage's services.

Intelligence

The app has some intelligence built into the vendor invoice workflow to help identify and set vendor names. The first time a user manually selects a vendor/contact, the application will remember the link between what was captured and what the user selected. For example, a user may have a

vendor called “Xerox Corporation”, but the invoice they scan in is captured as “Xerox”. If the user manually selects “Xerox Corporation” from their list of vendors, the app will note that “Xerox” and “Xerox Corporation” is the same thing. Next time they scan a similar invoice, the app can automatically fill the proper vendor.

The vendor name that was captured off the document will be stored per device. This value will not be linked to a user’s Sage account. This intelligence will also include an "edit distance" algorithm to find the closest match to account for spelling mistakes or captured values that are less than perfect.

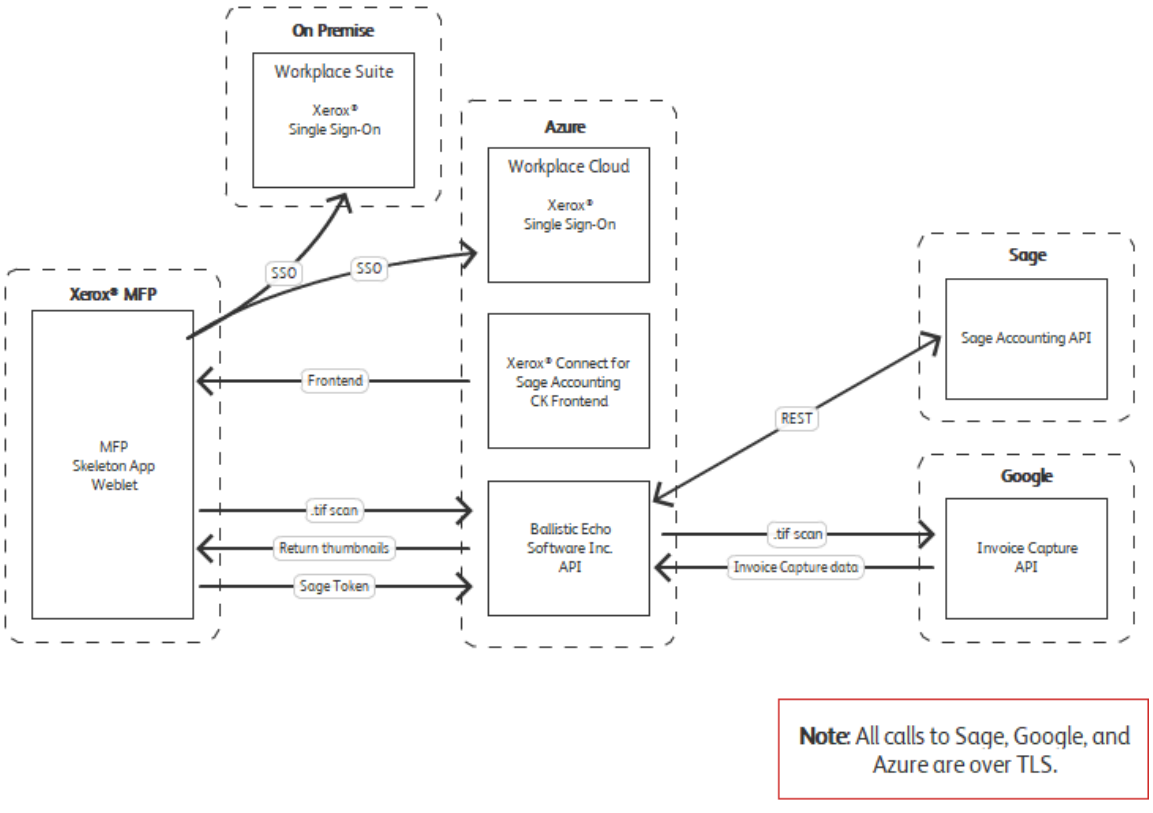
SNMP & Device Webservice Calls

During standard usage of Xerox Connect App for Sage Accounting, 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 local web service calls.

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

The Xerox Connect App for Sage Accounting 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 Connect App for Sage Accounting and the API require that the device can communicate over port 443 outside the client's network. All web communications between the API, Sage, Google, and Xerox devices are encrypted using HTTP Secure (TLS).

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.

Sales and vendor invoice information is transmitted, such as description, contact/vendor, and invoice total. If an invoice description is used, it could contain PII. The data itself isn't encrypted during transit, but it will be sent over TLS.

The thumbnails are stored using short live Secure Access Signature (SAS) URLs. Once the user is finished processing, the thumbnails are removed.

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

Table 1. 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/