Information Assurance Disclosure of Xerox® Connect App for QuickBooks Online

1. Introduction

Xerox® Connect App for QuickBooks Online (QBO) is a solution that connects Xerox® Multifunction Printers (MFP) to an individual's QuickBooks Online account. Scanning receipts and automatically having the receipt information processed and ready for review is easy. You can also conveniently add expenses and update transactions all from a Xerox® Multifunction Printer (MFP).

1.1. Purpose

The purpose of the Information Assurance Disclosure (IAD) is to disclose information for QBO 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 QBO 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® QBO does not establish security for any network environment.

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

1.2. 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 QBO app; as such, some user actions are not described in detail.

1.3. 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. Description and Details

2.1. Overview

The Xerox® QBO app consists of one primary workflow. The single workflow facilitates a combination of these steps:

- App hosting
- Authentication
- Selection
- Scanning
- Emailing
- SNMP & device webservice calls
- OCR & data extraction

2.2 App Hosting

The Xerox® QBO app consists of three key components; the device app, the API, and the portal. The device app is a ConnectKey® / EIP webapp and the API is a REST API. Lastly, the portal provides configuration management.

2.3. Authentication

Authentication consists of 2 key steps:

Portal authentication: The first step is to authenticate the user with Intuit by using the Xerox® Connect for QuickBooks Online portal which leverages Intuit's Single Sign-on (SSO). This can be done in a web browser on a computer. The user is prompted to enter their Intuit QuickBooks Online user-id and password to sign in. Once they have signed in, a QBO Oauth token is stored and encrypted in the Xerox® Connect for QuickBooks Online database.

Device authentication: Once a user has authenticated through the portal, the next step is to authenticate the device with the Xerox® Connect for QuickBooks Online portal. The user will be presented with the Settings screen where they will add the Xerox® device. They'll be presented with an activation code, which will need to be entered in the app when prompted. The device and portal will then share a secret going forward that only they know. This shared secret is stored locally on the device and in the database. It is encrypted in both locations.

2.4. Selection

At various steps in the application the user may be prompted to make selections. These selections include vendors and expense types. They are dynamic and are driven by API calls.

2.5. Scanning

When scanning, receipts are scanned and submitted to the API. Due to the nature of the Xerox® EIP scanning workflow design, the users scan is persisted. Then, processing, such as separation and thumbnail creation, is done on the scan itself. Once the processing has completed, it is handed to the API.

2.6. Emailing

When a new transaction is submitted through the app, the system will email the user's bookkeeper / accountant a URL that will take them to QuickBooks Online, where they can further review and modify the expense reimbursement. A copy of the expense details will also be emailed to the selected user for their own records.

2.7. SNMP & Device Webservice Calls

During standard usage of the QBO app, local calls to SNMP are initiated to pull relevant details such as device language and paper size preferences. The initiation of scan, print, and the usage of internal graphical components are handled though these local webservice calls.

2.8. OCR & Data Extraction

During processing, OCR and data extraction is run against the scanned receipt. Using the ABBYY API, characters and values are optically recognized on the scan, which is then extracted and used to automatically fill variables like date, total, and vendor.

3. Security

3.1. Hosting

The Xerox® QBO-API and the QBO 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

3.2. Secure Web Communications

All web communications between servers and Xerox® devices are encrypted using HTTP Secure (HTTPS).

3.3. Encryption

The user's OAuth token is persisted and encrypted in the API database. While at rest, this token is salted and encrypted using AES-256. Token encryption and decryption is done on the server. The Xerox® device has no internal means to decrypt this value.

3.4. Data

Receipts 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. Orphaned items (user didn't complete the transaction) are removed multiple times per hour. A receipt also constitutes metadata about the receipt. It includes items such as amount, date, notes, vendor ID (number from QBO), etc.

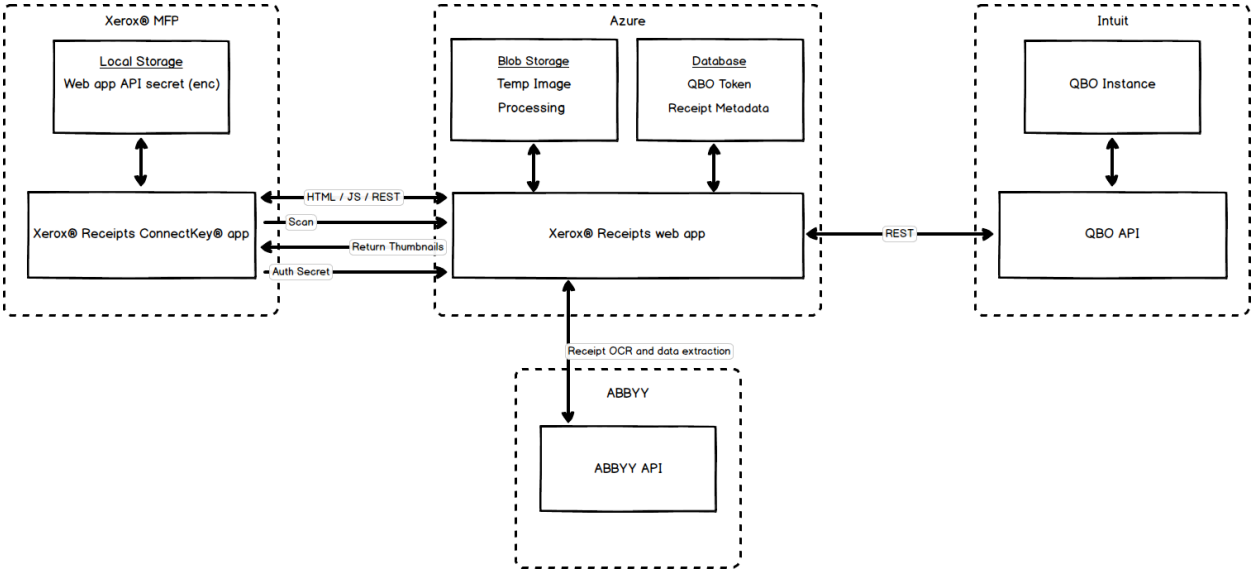
During the processing of a scanned receipt, a receipt bundle is stored. All detail about the receipt, such as data from OCR, images, and any details that a user may key in on the device, is temporarily persisted. Once the user has finished, all receipt details are deleted.

3.5. Single Sign-On (SSO)

Please note that the QBO app should always be used on a secure network. The app uses Intuit's SSO, which means it is limited by any of the security features Intuit has in place.

3.6. Data Flow Diagram

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



4. Ports

4.1. App & API

The Xerox® QBO app and QBO-API require that the device can communicate over port 443 outside the client's network.