Xerox® Security Guide

Connect for XMPie®

xerox™

Document Version: 1.0 (September 2019).

Contents

1. Introduction

Purpose

The purpose of the Security Guide is to disclose information for Xerox apps 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 the Xerox apps 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 the Xerox apps do not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity or Xerox 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. General Security Protection

User Data Protection within the products

Document and File Security

File content is protected during transmission by standard secure network protocols at the channel level. Since document source content may contain Personally Identifiable Information (PII) or other sensitive content, it is the responsibility of the user to handle the digital information in accordance with information protection best practices.

Hosting - Microsoft Azure

The cloud services are hosted on the Microsoft Azure Network. The Microsoft Azure Cloud Computing Platform operates in the Microsoft® Global Foundation Services (GFS) infrastructure, portions of which are ISO27001-certified. Microsoft has also adopted the new international cloud privacy standard, ISO 27018. Azure safeguards customer data in the cloud and provides support for companies that are bound by extensive regulations regarding the use, transmission, and storage of customer data.

The Apps hosted in the cloud are scalable so that multiple instances may be spun up/down as needed to handle user demand. The service is hosted both in the US and Europe. Users will be routed to the closest server geographically based on server load and network speed.

Cloud Storage – Microsoft Azure

All Azure Storage and Azure SQL data is secured when at rest using AES-256 encryption.

For a full description, please follow these links:

Azure SQL
https://azure.microsoft.com/en-us/updates/newly-created-azure-sql-databases-encrypted-by-default/

Azure Storage
https://azure.microsoft.com/en-us/blog/announcing-default-encryption-for-azure-blobs-files-table-and-queue-storage/

Xerox® Workplace Suite/Cloud and Single Sign-On Services

The Xerox® ConnectKey App Single Sign-On feature integrates with the Xerox® Workplace Suite/Cloud authentication solution to store user access information for SSO-compatible Xerox Gallery Apps. After the user enters their storage service credentials the first time, the XWS/C solution acts a storage vault where the login information is securely stored.

All content to be stored in the vault is encrypted with AES 256 by the SSO Manager server before being given to the SSO vault that resides on the XWS/C solution. This ensures that the SSO vault can never view or use the contents being stored in the vault. Only the SSO Manager infrastructure knows how to decrypt the content stored in the vault and only the App knows how to use it.

The SSO Manager service manages the encryption key exchange required for secure communications and encrypts/decrypts the content saved in the vault.

For a full description, please review the Xerox® Workplace Suite/Cloud Information Assurance Disclosure: https://security.business.xerox.com/en-us/products/xerox-workplace-suite/

User Data in transit

Secure Network Communications

The web pages and app services that constitute the Xerox solution are deployed to Microsoft Azure App Services. All web pages are accessed via HTTPS from a web browser. All communications are over HTTPS. Data is transmitted securely and is protected by TLS security for both upload and download. The default TLS version used is 1.2.

The Xerox® app requires the user to provide proper/valid credentials in order to gain access to the application's features. Authenticated users are allowed to access the features and data using HTTPS.

At launch, the apps must get an authentication/session token through the solution's authentication process. The access token acquired is used for that session of the app.

When using the ConnectKey App installed on a Xerox device, if the customer environment includes an Authentication solution (e.g., Xerox® Workplace Suite/Cloud) with Single Sign-On functionality enabled, the user can agree to have their user credentials securely stored and automatically applied during subsequent app launches.

All communication is done via HTTPS and the data is transmitted securely and is protected by TLS security. The default TLS version used is 1.2. Xerox App Gallery supplies a link to a Certificate Authority root certificate for validation with the cloud web service. It is the responsibility of the customer to install the certificate on their devices and to enable server certificate validation on the devices.

For more information related to Azure network security, please follow the link: https://docs.microsoft.com/en-us/azure/security/azure-network-security

Xerox Workplace Suite/Cloud and Single Sign-On Services

The Xerox Workplace Suite/Cloud server accepts credential storage requests from the App via the SSO Manager service (the ConnectKey App retrieves a vault key from the SSO Manager and uses it to retrieve login credentials from the XWS/C service). All communication is via HTTPS and the data is transmitted securely and is protected by TLS security. The default TLS version used is 1.2

3. Xerox® Connect for XMPie® App – ConnectKey App

Description

Overview

ConnectKey App
The ConnectKey App enables users to browse, customize, and print XMPie Print-on-Demand products. The app assists the user with:

1. Browsing documents and other print products available through an XMPie storefront
2. Selecting and optionally customizing the print product.
3. Printing the document on the Xerox device.

Table 1. ConnectKey App user benefits

Application	What can I do?
ConnectKey App	• Login to my XMPie account (optional) • Browse product categories and lists • Select a document or other print product • Customize the product (optional) • Print on the Xerox device.

App Hosting

The ConnectKey App depends heavily on cloud hosted components. A brief description of each can be found below.

ConnectKey App
The ConnectKey App consists of two key components, the device weblet and the cloud-hosted web service. The device weblet is a ConnectKey/EIP web app that enables the following behavior on a Xerox device:

1. Presents the user with an application UI that executes functionality in the cloud.
2. Interfaces with the EIP API, which delegates work, such as document scanning and printing.

The weblet communicates with the cloud-hosted web service, which executes the business logic of the app.

XMPie Web Service
The solution integrates to the XMPie Print-on-Demand service using the XMPie REST API. The app makes API calls to retrieve the list of available product categories and products, select customization options, and download the final print-ready files. All requests are made over HTTPS.

Single Sign-On via Xerox® Workplace Suite/Cloud and SSO Manager
In order to improve user experience, by removing the need to log in to the ConnectKey App each time Xerox offers an optional Single Sign-On (SSO) capability. Users can log into the printer and are then able to launch the app without the need to provide additional credentials.

Xerox Extensible Interface Platform® Web Services

During standard usage of the ConnectKey App, calls to the device web services are used to initiate and monitor scan functions and to pull relevant details related to device properties and capabilities.

Components

MFD with Xerox® Connect for XMPie App – ConnectKey App

This is an EIP capable device that can print and execute ConnectKey Apps installed from the Xerox App Gallery. In this case, the device has the Xerox® Connect for XMPie App installed.

Xerox® Connect for XMPie App – Web Services

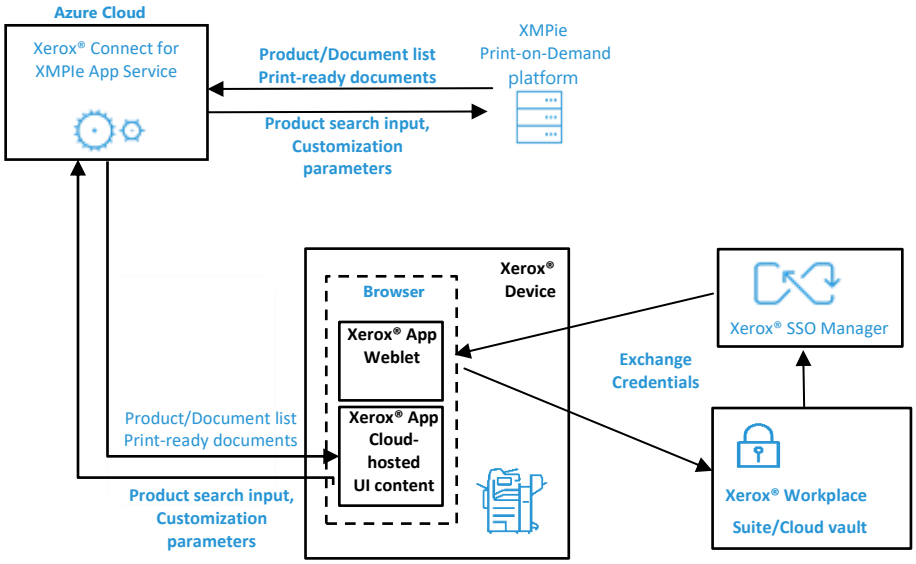
The Web Service is a service hosted on the Microsoft Azure Cloud System. The service is responsible for hosting the web pages which are displayed on the UI of the printer and provide the services support for the Xerox® apps. The web service interacts with XMPie services using the XMPie REST APIs and Microsoft services using the Azure APIs.

XMPie

The XMPie cloud hosted service provides a web API that is used for retrieving documents and other print products, specifying customization options, and downloading print-ready files.

Architecture and Workflows

Data Flow Diagram



Workflows

Print – Browse available XMPie documents, print on local device

Step 1: Launch the App on the Xerox device.

Step 2: Login with XMPie account credentials to view the Main page. (Optional)

Step 3: Browse the list of product categories, select a product to print

Step 4: If the product is customizable, specify the desired values.

Step 5: Preview the customized (or static) print-ready images.

Step 6: Print the document(s) using the Print button.

User Data Protection

Application data stored in the Xerox cloud

User data related to the categories below are stored temporarily in cloud storage during communication with the XMPie service. No data is stored persistently in the cloud.

- Login to XMPie account
- Print product descriptions and preview images
- Customization options for print products

The following activities will trigger a delete event, for digital document files that meet the associated criteria.

- A delete occurs when the system detects intermediate processing files exist after a job has completed.
- Closing the app.

App usage data, that is unrelated to user Personally Identifiable Information, may be stored indefinitely for event reporting purposes.

Local Environment

Application data transmitted
Application data related to the categories below are transmitted to/from the Xerox device.

- Account data
- Session data
- Job data

Application data stored on the Xerox device
The following app data is stored on the device, in persistent storage, until the App is uninstalled from the device.

- None

HTTP Cookies
The ConnectKey App does not store any cookies on the device.

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

Table 4. 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/