Software Version 5.0
Version 1.0
June 2019

Xerox®
Security Guide
for
Xerox® Workplace App

Table of Contents

1. Introduction

The Xerox® Workplace Application is an application designed to run on mobile phones and tablets, allowing users to connect to their network printers for a simple convenient method of printing. The app is designed to work with the Xerox Workplace Solutions:

- Xerox® Workplace Suite
- Xerox® Workplace Cloud

The Xerox® Workplace Application can also be run as a stand-alone printing and scanning solution that does not require any interfacing or interaction with the Xerox® Workplace Suite/Cloud. When running in this mode, the app enables mobile printing to many Xerox printers and multi-function devices without the need for third party apps or additional print drivers. Easily print photos, web pages and documents when your mobile device is connected to a compatible Xerox printer through a wireless network. Control print settings including color, number of copies, paper orientation, staples, secure code release printing, and more. In addition to printing, the Xerox® Workplace App also supports scanning from a Xerox multi-function to the mobile device using through a wireless network. This provides an easy mechanism to get hard copy documents into an electronic format on your phone, where they can easily be shared or modified.

Purpose

This Information Assurance Disclosure (IAD) focuses on the stand-alone printing solution provided by the Xerox® Workplace Application. For details on the use of this application with the mentioned solutions: Xerox® Workplace Suite/Cloud, please refer to the IADs of each respective product.

The purpose of the Security Guide is to disclose information for Xerox® Workplace App with respect to application security. Application 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® Workplace Cloud 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® Workplace Cloud does not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity or Xerox® Workplace 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 solution; 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

The Xerox® Workplace Application for iOS® and Android™ enables printing to many Xerox printers and multi-function devices without the need for additional print drivers. It also supports scanning a document from a Xerox® multi-function device to your mobile device. You can find and print/scan to Xerox printers or multifunction printers that are on a wireless network by downloading the Xerox® Workplace App from the Google Play™ store or the Apple App Store®.

Component Diagram

The architecture of the Xerox® Workplace Application incorporates technical controls to eliminate, where possible, information security risk from all information assets including software components, connected system components, and information owners. The Xerox® Workplace App Architecture illustrates the relationship between the Xerox® Workplace Application and these other system components.

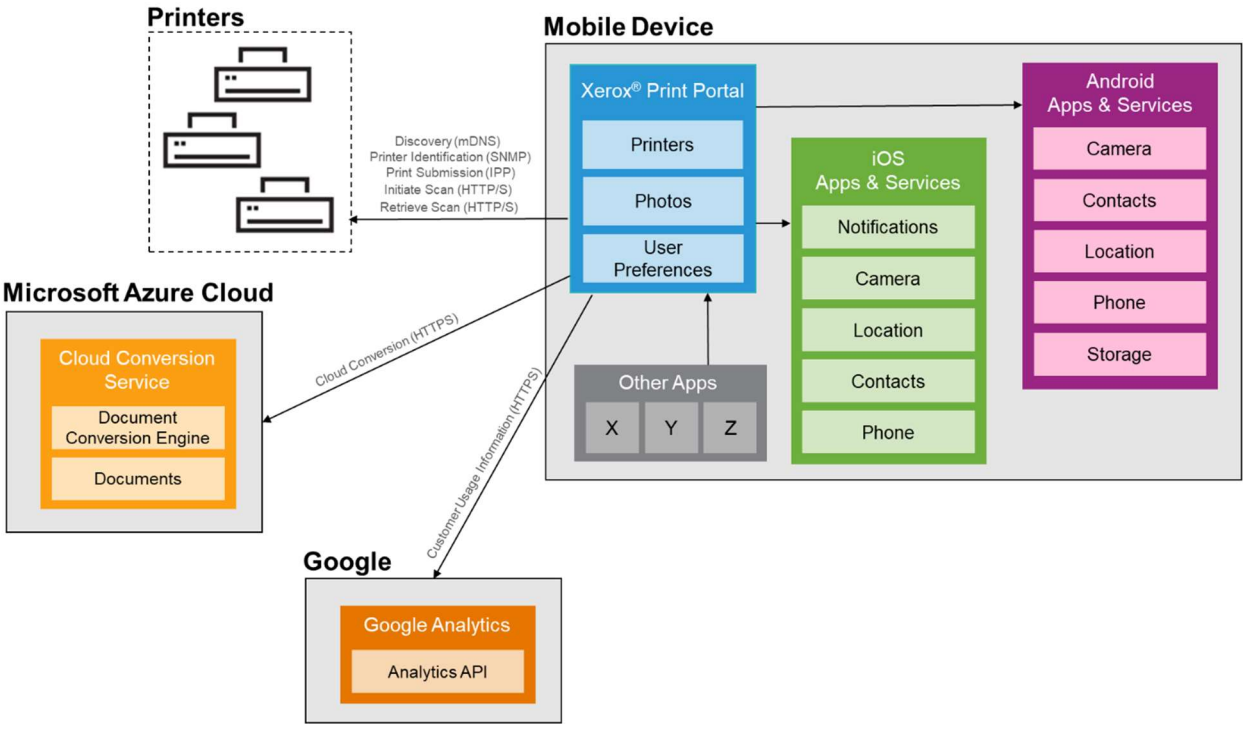

Figure 2.2-1: Component Diagram

Description of System Components

Component	Description
Mobile User	End user using Android/iOS device with the Xerox® Workplace App.
Xerox® Workplace App	Mobile Phone app that allows the user to find printers and submit print and scan jobs.
Xerox® Workplace App Local Storage	Used to store information about the discovered printers, and user preferences (e.g. for Google Analytics or HTTPS scanning).
Android Provided Apps and Services	Xerox® Workplace App makes use of services on the mobile device. These vary slightly by platform. Android: Camera, Contacts, Location, Phone, Storage. IOS: Camera, Location, Notifications, Phone, Contacts. Permission must be granted by the user to use these services. Many of the permissions are only requested at the time of need.
Other Apps	When printing, users selecting a document or file from within any App that supports “share with” (Android) or “open in” (iOS), and the mime type of the selected document is supported by the Xerox® Workplace App, then the user will be able to select Workplace App from within the other App. For scanning, users can drop the scanned document to any applications installed on the phone that support “share with” or “open with” for PDF files.
Printer	Printer used for printing jobs which are output from the Xerox® Workplace App or scanning jobs to the mobile device. The printer must support IPP.
Cloud Conversion Service	If the user is attempting to print a file that is not in print ready format, then the Xerox® Workplace App will use an Azure hosted Cloud Conversion Service to convert the file to a print ready format.
Google Analytics	If the user enables Google Analytics, then the App will collect non-sensitive usage information and will push this up to Google. This information provides Xerox with an understanding of how customers are using the app and can influence new features and functionality added in the future.

Table 2.3-1: System Components

3. System Architecture

Sub-Systems

Xerox® Workplace App

Memory Information (SoV)

Volatile Memory					
Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Information	Process to Clear:
RAM	Varies	Y	Executable code, temporary storage	Yes	Power Off; Process Cleanup

Table 3.1.1.1-1: Xerox® Workplace App Volatile Memory

Non-Volatile Solid-State Memory					
Type (Flash, EEPROM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Information	Process to Clear:
Mobile Phone Storage	N/A	N	Discovered printer information and user preferences (for Google Analytics)	Yes	Deletion of App to remove Configuration and App Content.

Xerox 3.1.1.1-2: Xerox® Workplace App Non-Volatile Memory

Cloud Conversion Service

Memory Information (SoV)

Volatile Memory					
Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Information	Process to Clear:
Azure storage – System Memory	Varies	Y	Executable code, temporary storage, username of logged in user	Yes	Power Off; Process Cleanup

Table 3.1.2.1-1: Cloud Conversion Service Volatile Memory

Non-Volatile Solid-State Memory					
Type (Flash, EEPROM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Information	Process to Clear:
HDD Array	N/A	N	Original and converted documents to be printed.	Yes	Requires removal of Xerox roles. Job data is cleared based on job retention timers.

Xerox 3.1.2.1-2: Cloud Conversion Service Non-Volatile Memory

4. System Interaction

System Components

Xerox® Workplace App

The Xerox® Workplace App is an Android/iOS App, which supports printing of many common file types, as well as scanning documents from a Xerox® multi-function printer to the mobile device. Access to the Xerox® Workplace App will be controlled by the mobile device's authentication mechanism. From within the App, Users may select files (iOS: Files, Photos, Email or Camera; Android: File Library, Clipboard, Web Page or the Camera) to be printed. They may also select a printer from which to initiate a scan request and store the job locally on the phone or using another filing-based App such as Microsoft® OneDrive.

The Xerox® Workplace App provides the following functions:

- Allows discovery or identification of printers via multi-cast DNS, QR Code scanning or NFC.
- Supports the ability to convert documents or files to a print ready format using a Cloud based conversion service. All communication with the Cloud Conversion Service is done using HTTPS over port 443. Transport Layer Security (TLS) cryptographic protocols are used for all communication to the Cloud Conversion Service.
- Submits print ready files to the selected printer via the IPP/S protocol.
- Submits scan requests to the selected printer and retrieves the scan file, where it can then be stored on the local phone or the user can drop the scanned document to any applications installed on the phone that support "share with" or "open with" for PDF files.
- Collects non-sensitive user information (if enabled) and uploads this to a Xerox account using Google Analytics. All data collected is anonymous and is collected in an aggregate form such that any information collected cannot be associated with an individual. No PII (Personally Identifiable Information) is collected.

Xerox® Workplace App Local Storage

The following data is stored in the Xerox® Workplace App's assigned storage space on the mobile device. This is typical of all mobile apps. Other apps do not have access to this same space on the mobile device. The collection of stored information includes:

- Discovered Printers – Printer manufacturer, model, IP address, printer name, location, status, supported print options (color, 2-sided, etc.).
- User Preferences – Google Analytics enablement setting, encryption preference (use HTTPS when available), application logs (for debugging).

The Xerox® Workplace App uses iOS/Android approved methods to encrypt and secure information stored on the device.

- If the mobile device is password protected by the user, then the Xerox® Workplace App data is encrypted and secure.
- [iOS Only] If the mobile device is NOT password protected by the user, then the Workplace App data is NOT encrypted and can be easily accessed by connecting the mobile device to a PC and browsing the files in a file browser. In fact, all data from all apps using this security model are vulnerable in the same manner.

Android Provided Services

The Xerox® Workplace App may acquire data from the following services provided by the OS on the mobile device:

- Camera
- Contacts
- Location (not used for local printing / scanning)
- Phone (not used for local printing / scanning)
- Storage

The user is asked to grant/deny permission to access these services/data stores when or if they are needed based on the features being used. The user does not need to grant permission for any of these services when the app is installed. The user can change their decision to grant/deny permission through Settings on their mobile device. Access to each of these services is managed individually.

Access to Contacts is used to retrieve the logged-on user of the mobile device (i.e. their Google username/email). This information is used as the user identity when submitting jobs to the printer. Typically, you will see this name show up on the banner sheet of the print job. The username is only stored in RAM while the app is running.

The Camera is used for printer identification. In addition to discovering printers on the Wi-Fi network, the Xerox® Workplace App can also discover a printer if the devices QR identification code is scanned, or using the built-in NFC feature on some models of printers (e.g. AltaLink and VersaLink).

Location and Phone are not used for local printing. Users must be logged into one of the following Xerox solutions in order to make use of the Location and/or Phone service:

- Xerox® Workplace Suite
- Xerox® Workplace Cloud

iOS Provided Services

The Xerox® Workplace App may acquire data from the following services provided by the OS on the mobile device:

- Notifications
- Camera
- Location
- Contacts
- Phone (not used for local printing / scanning)

The user is asked to grant/deny permission to access Notifications and Location when the app is installed. The user can change their decision to grant/deny permission through Settings on their mobile device. Access to each of these services is managed individually.

The Camera is used for capturing images for printing as well as for printer identification. In addition to discovering printers on the Wi-Fi network, the Xerox® Workplace App can also discover a printer if the devices QR identification code is scanned, or using the built-in NFC feature on some models of printers (e.g. AltaLink and VersaLink).

Interaction with Other Installed Apps

Users may access the Xerox® Workplace App from within other applications. After selecting a document or file from within any App, if that App supports both of the following, then the user will be able to select the Xerox® Workplace App from within the other App.

- The app must support “share with” (on Android) or “open in” (on iOS).
- The mime type of the selected document must be supported by the Xerox® Workplace App.

This will provide access to the selected document / file from within Workplace App so that it may be printed at any available printer.

When performing a scan job, the resulting file retrieved from the printer may be stored in local storage of the mobile device (e.g. Files). Alternatively, it may be shared with an App that supports sharing of files via the Operating System of the mobile device.

Printers

The Xerox® Workplace App can interact with any Xerox printer that supports the necessary Discovery, Identification, Print Submission and Scanning interfaces.

Discovery

Discovery of Xerox printers uses Multi-Cast DNS (Domain Name System), over port 5353. Printers can also be discovered manually by these methods: Users can enter the IP address or DNS name of the printer, they may scan a QR code or they may use NFC discovery. All these methods of discovery will then try to contact the printer over IPP and is successful, the printer will be added to the discovered printer list.

Identification

Once a printer has been discovered the Xerox® Workplace App will obtain the printers sysObjID using SNMP (Simple Network Management Protocol) over ports 161 and 162. This information is only used when printing documents that require conversion via the Cloud Conversion Service.

Print Capabilities and Submission

Determination of the printer capabilities, such as supported print options or supported PDLs (PDF, PS, PCL) as well as the actual submission of the print job is done using IPP (Internet Printing Protocol) over port 631.

Scan Capabilities and Submission

Determination of the printer scan capabilities, as well as the actual scan submission and retrieval of the resulting file is over HTTP/HTTPS. The user can configure the App to always use HTTPS. By default, the app will use HTTPS (port 443) when available and fall back to HTTP (port 80) if not supported.

Mobile User

The mobile user is an end-user attempting to print a file using the Xerox® Workplace App running on a mobile device. It is assumed that the client's security policy and systems have already authorized the user to access and use corporate resources (e.g. network, multi-function device).

Cloud Conversion Service

The Cloud Conversion Service is hosted in the Microsoft Azure Cloud. This service allows the Xerox® Workplace App to upload files which are not in print ready format (e.g. a photo), it will then convert them into a print ready format (PS or PCL) and allows the App to retrieve them. Assess to the Cloud Conversion Services is Xerox password protected. The Xerox® Workplace App uses the HTTPS over TLS protocol on port 443 for all communication with the Cloud Conversion Service. It establishes an HTTPS secure connection with the Cloud Conversion Service relying on the mobile device operating system to validate the security certificate as part of establishing the TLS connection. The security certificate is issued by Comodo (a trusted certificate authority) and ensures that the application has been verified and validated.

The Windows Azure Platform operates in the Microsoft® Global Foundation Services (GFS) infrastructure, portions of which are ISO27001-certified.

Windows Azure Security Highlights:

- Built-in Identity Management for administrator access
- Dedicated hardware firewall
- Stateful packet inspection technology employed
- Application-layer firewalls
- Hypervisor firewalls
- Host-based firewalls
- SSL termination / load balancing / application layer content switching
- Each deployed hosted service is segmented in its own VLAN, preventing compromised node access

Please visit the following Microsoft web sites for more information:

- Windows Azure Security Overview:
  http://azure.microsoft.com/blog/2010/08/10/new-windows-azure-security-overview-white-paper-now-available/

  Select Windows Azure Security Overview.
- Microsoft Azure Trust Center:
  https://azure.microsoft.com/en-us/support/trust-center/

Google Analytics

Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. In this case, the Xerox® Workplace App is using it to track usage and access information related to the App. This feature is optional and the user may choose to disable the sending of this information if desired. There is no customer or user sensitive information being collected. The app will track a small set of metrics like the number of pages, copies and printer model used to analyze usage. This will be done completely anonymously and cannot be associated with any individual since no PI (Personal Information) is collected. Google may track additional information like device model used, IP address by default. Refer to Google's privacy policy https://www.google.com/intl/en/policies/privacy/ for further details.

All data collected by the Xerox® Workplace App is accessible only to Xerox authorized personnel and is used to better understand how users are using the app. This information is used to plan future features and software changes of the app to better tailor it to the needs of our customers.

All communication between the Xerox® Workplace App and the Google Analytics service is done via HTTPS over TLS on port 443.

5. Logical access, network protocol information.

Protocols and Ports

The following table shows the protocols and typical port numbers used in the Xerox® Workplace App:

Protocol (Ports)	Protocols / Ports
mDNS (port 5353)	Device Discovery
IPP (port 631)	Printer Status, Capability and Print Submission
SNMP (port 161)	Device Identity
HTTPS (443)	Document conversion to print ready format and retrieval. Scanning: detection, initiation and retrieval. Google Analytics
HTTP (80)	Fallback for scanning: detection, initiation and retrieval.

Table 5.1-1: Protocols and Ports

6. Additional Information & Resources

Security @ Xerox®

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see http://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: http://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	http://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/