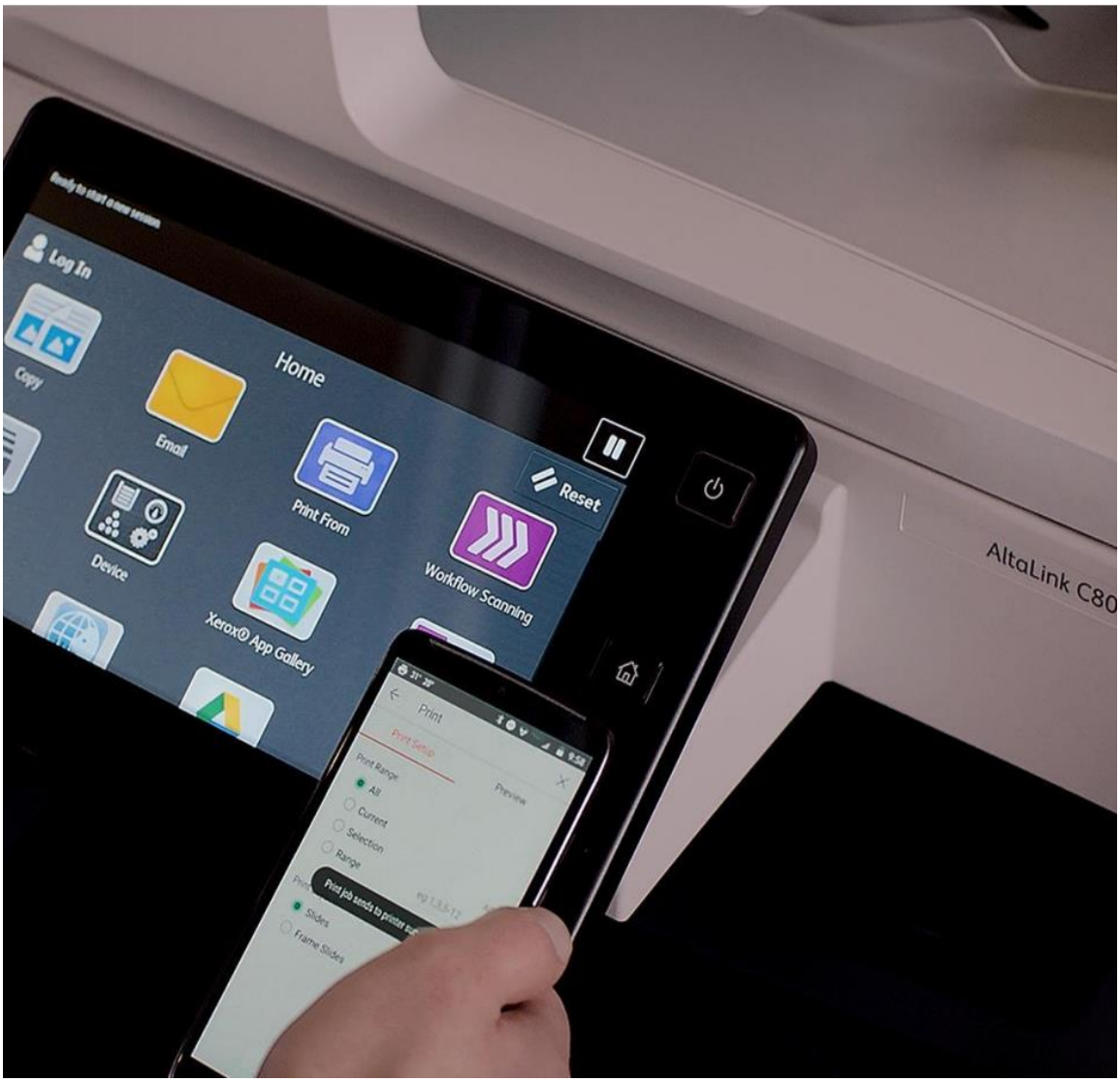
Security Guide

Xerox® Scan to Cloud Email App



Document Version: 1.0 (March 2021).

Contents

1. Introduction 1-1

Purpose 1-1

Target Audience 1-1

Disclaimer 1-1

2. Product Description 2-2

Overview 2-2

App Hosting 2-2

Components 2-2

Diagram 2-4

Data flow Diagram 2-4

Workflows 2-5

Device Authentication 2-5

App Startup 2-5

Manage a stored list of recipients 2-5

Manually enter email addresses 2-5

Select email addresses from a stored list of recipients 2-5

Scan a hard copy document 2-5

User Data Protection 2-6

Application data stored in the Xerox cloud 2-6

Local Environment 2-6

PII data Management 2-6

Clearing Device Browser Cache 2-7

3. General Security Protection 3-8

User Data Protection within the Products 3-8

Document and File Security 3-8

Hosting - Microsoft Azure 3-8

Cloud Storage – Microsoft Azure 3-8

Xerox® Workplace Suite/Cloud and Single Sign-On Services 3-8

User Data in Transit 3-9

Secure Network Communications 3-9

Xerox Workplace Suite/Cloud and Single Sign-On Services 3-9

4. Additional Information & Resources 4-10
Security @ Xerox 4-10
Responses to Known Vulnerabilities 4-10
Additional Resources 4-10

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. Product Description

Overview

The Xerox® Scan to Cloud Email App consists of a limited number of workflows. The workflows supported are:

- Scanning a hard copy document and emailing it to a recipient
- Selecting recipients from a list of contacts saved in the App, on the device

Completing a workflow involves a combination of the following aspects described in detail below.

- App Hosting
- App Startup
- Manage a stored list of recipients
- Manually enter email addresses
- Select email addresses from a stored list of recipients
- Scan a hard copy document

APP HOSTING

The Xerox® Scan to Cloud Email App depends heavily on cloud hosted components. A brief description of each can be found below.

Xerox® Scan to Cloud Email App

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

- Presents the user with an application UI that executes functionality in the cloud.
- Interfaces with the EIP API, which delegates work, such as querying device details and initiating a scan.

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

Send Email Service Middleware

The web tier component hosting the app communicates directly with a Send Email service, which securely facilitates submitting the email to SendGrid on Azure over SMTP/TLS.

Xerox Extensible Interface Platform®

During standard usage of the Xerox® 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® Scan to Cloud Email App – ConnectKey App

This is an EIP capable device that can print, scan and execute ConnectKey Apps installed from the Xerox® App Gallery. In this case, the device has the Xerox® Scan to Cloud Email App installed.

Xerox® Scan to Cloud Email App Web UI

The Web UI component is a service hosted on the Microsoft Azure Cloud System. The Web UI component is responsible for hosting the web pages, which display on the UI of the printer.

Xerox® Scan to Cloud App – Service Interface

The Service Interface component is a service hosted on the Microsoft Azure Cloud System. The Service Interface provides the business logic service and interfaces with the Send Email Service Middleware.

Send Email Service Middleware

The Send Email Service Middleware component is a service hosted on the Microsoft Azure Cloud System, which interfaces with the SendGrid on Azure connector on the App's behalf.

SendGrid on Azure Connector

SendGrid on Azure is a global, custom-built Mail Transfer Agent architected for the cloud and supported by a redundant, self-hosted datacenter infrastructure.

Xerox App Gallery

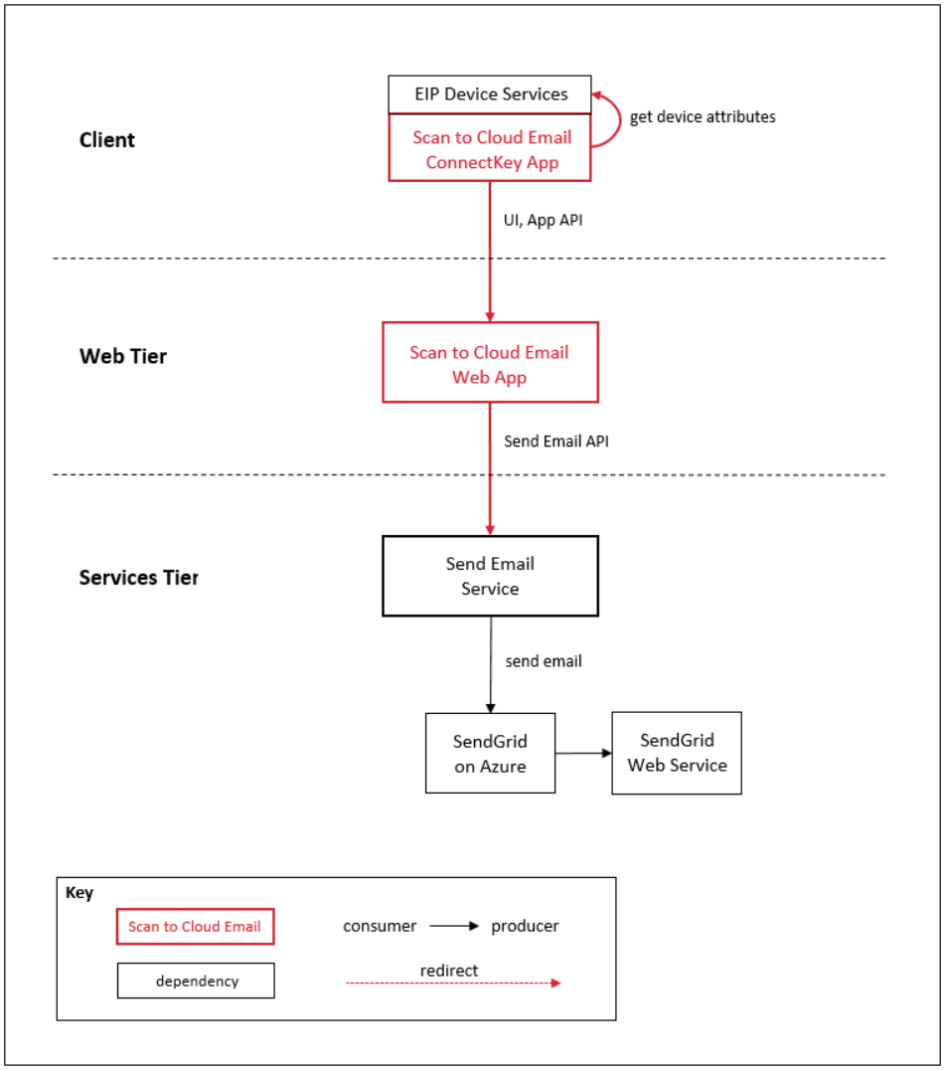
The App Gallery component is a web application, with services, hosted on the Microsoft Azure Cloud System. The App Gallery is accessed to ensure the Application is entitled to run and is used when upgrading the App whenever the auto-update conditions apply.

SendGrid Service

SendGrid is a cloud-based email service that provides reliable transactional email delivery, scalability.

Diagram

DATA FLOW DIAGRAM



Workflows

DEVICE AUTHENTICATION

Device login: Prior to starting the Xerox® Scan to Cloud Email App, users may sign-in at the MFD using their networks credentials.

The device login interaction is confined to the device login workflow, and the credential values provided are not interrogated by the Xerox® Scan to Cloud Email App.

APP STARTUP

During startup of the Xerox® Scan to Cloud Email App, the main page initialization script calls the App Gallery API to get the app installation's entitlements.

Once entitlements are verified, the main page initialization script executes local HTTP calls to device EIP web services in order to obtain relevant details associated with the device and its capabilities (i.e. Device Serial Number, MAC Address, device generation etc.).

During app initialization, the EIP browser runs the HTML and JavaScript delivered to the device, which renders the App UI content retrieved from app endpoints hosted in the Azure App Service.

MANAGE A STORED LIST OF RECIPIENTS

Users may manage a shared list of up to 50 email addresses that's accessible to all users. The app encrypts the email addresses that are saved using a symmetric key before storing them in local persistent storage. The algorithm and key size used is AES-256.

MANUALLY ENTER EMAIL ADDRESSES

Users may populate the email distribution list manually.

SELECT EMAIL ADDRESSES FROM A STORED LIST OF RECIPIENTS

Users may populate the email distribution list by selecting one or more email addresses within the saved recipients list.

SCAN A HARD COPY DOCUMENT

After confirming the scan settings and any other user specified job attributes, users may scan their document, which will automatically send a digitized version of the hard copy to recipients that are included in the job's distribution list.

The app encrypts send email requests travelling over the wire to the SendGrid on Azure connector using TLS 1.2, and the email is sent to the SendGrid service over an SMTP relay using TLS over well-known ports.

User Data Protection

APPLICATION DATA STORED IN THE XEROX CLOUD

User data related to the categories below are stored in cloud persistent storage until a delete event occurs.

- Create a scanned image file from a paper document and email to recipient(s).

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.

The balance of data stored in the cloud, 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.

- Session data
- Job data
- Email 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.

- Device data
- Configuration data
- Saved email addresses

The app encrypts the email addresses that are saved using a symmetric key before storing them in local persistent storage. The algorithm and key size used is AES-256.

HTTP Cookies

The Xerox® Scan to Cloud Email App does not store any cookies on the device.

PII DATA MANAGEMENT

The following personal data is acquired, transmitted, and potentially stored by the Xerox® Scan to Cloud Email App.

- Email addresses

Clearing Device Browser Cache

The Device Browser Cache is cleared when one of the following events occur.

- Device Logout
- Device Timeout
- Double Clear All
- Browser Restart

Cycling the Browser from Disabled to Enabled

3. 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 data is secured when at rest using AES-256 encryption.

For a full description, please follow these links:

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® Solutions 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 Xerox® Scan to Cloud Email 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, no additional administrative steps will be required to operate the app, since the app does not support user personalization.

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 Xerox® 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.

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

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 Additional Resources